VICTORIA

Victorian
Auditor-General

Implementation of the Criminal Justice Enhancement Program (CJEP)

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
June 2008

PP No 106, Session 2006-08

ISBN 1 921060 71 9

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

The Hon. Robert Smith MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Jenny Lindell MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report on *Implementation of the Criminal Justice Enhancement Program (CJEP).*

Yours faithfully

DDR PEARSON
Auditor-General

11 June 2008

Foreword

The Criminal Justice Enhancement Program (CJEP) is a highly complex major information technology project of the Department of Justice (the department).

Its aim was to improve the information systems environment that supports the administration of criminal justice within Victoria. It was approved in October 1998 with funding of $14.5 million and a target completion date of November 2000.

CJEP has produced benefits, but it has not been implemented on time or on budget. Four of the five CJEP projects have been delivered but the electronic brief/disclosure project (E*Brief) is not operating and may not be fully implemented until 2009.

There were substantial cost overruns on CJEP. The department spent $39.9 million on CJEP's development and implementation to May 2008, and Victoria Police estimates that a further $4 million will be required to complete the E*Brief project.

Determining and securing adequate funding is crucial to the success of any project. The CJEP experience clearly demonstrates that there was a failure to identify and secure sufficient funding at the outset. This can be attributed to an inadequate business case, which contributed to poor scoping of the project and a failure to identify realistic funding requirements.

It was also evident that the complexity, magnitude and level of cross agency involvement required were underestimated. This is a particular challenge for any multi-agency implementation and demands due consideration of what is an appropriate contingency in planned timelines and costs.

The implementation of CJEP has been overseen by a steering committee comprising representatives from the key agencies involved in CJEP, and its timely and successful completion was partly dependent on these partner agencies. The audit found fluctuating levels of commitment to and ownership of CJEP by partner agencies and that the CJEP Steering Committee did not have the authority to compel commitment and ownership by agencies, its powers were essentially persuasive. This warrants consideration in developing governance frameworks for future projects of this nature.

DDR PEARSON
Auditor-General

11 June 2008

Contents

1 Executive summary

1.1 Introduction

The Criminal Justice Enhancement Program (CJEP) is a highly complex major information technology project of the Department of Justice (the department). It is an integrated Information and Communication Technology (ICT) platform designed to support the participation of the key law enforcement agencies engaged in the administration of criminal justice within Victoria. It includes Victoria Police, the Office of Public Prosecutions, Victoria Legal Aid, the County Court and Corrections Victoria.

CJEP is designed to integrate and streamline systems and processes across agencies to minimise transaction costs and to improve access, quality and timeliness of information to agencies, courts, legal practitioners and the public.

CJEP was approved to proceed in October 1998 with funding of $14.5 million and a target completion date of November 2000. Originally, the CJEP program scope comprised five principal projects. Three additional projects were subsequently added.

The CJEP projects have been incorporated into the following three key integrated IT software applications:

- **E*Justice—**to be used by police, prosecutions, corrections and legal aid officers, with a focus on managing information about accused persons and handling briefs of evidence
- **ACS Courts—**to be used by the County and Magistrates' Courts with a focus on improving case management and sentencing information
- **Justice Knowledge Exchange—**to manage the exchange of selected data between E*Justice, ACS Courts, and the legacy IT systems that remain in operation in justice agencies.

The CJEP systems are referred to collectively as the Integrated Justice Systems suite of applications or the Integrated Justice Systems (IJS). The CJEP systems operate in conjunction with a large number of legacy systems and reside in a complex set of networks in Victoria Police and the department. IJS also includes secure links between the department, Victoria Police, Office of Public Prosecutions, Corrections Victoria and private prison providers to enable the sharing of information.

The Secretary of the department is the CJEP project sponsor and responsibility for day to day project management of CJEP has rested with the department. Implementation of CJEP has been overseen by a steering committee comprising representatives from the key agencies involved in CJEP.

The department appointed a primary IT contractor in November 2000 to scope, design, build, install and support CJEP applications. This contract concluded in December 2005. At that time, a unit was established within the department's Technology Services Group to maintain, support and enhance CJEP applications into the future.

In May 2003 our Office reported to Parliament on the progress of CJEP and the adequacy of its management at that time. That report outlined the main achievements under CJEP, the widening of its scope and funding and its then target completion date of March 2004. This revised target completion date was not achieved.

1.2 Implementation of CJEP

CJEP has not been implemented on time or on budget. While four of the five CJEP projects have been delivered it is not complete because the electronic brief/disclosure project (E*Brief) is not operating and may not be fully implemented until 2009.

The department considers CJEP to be complete because in its view CJEP's core IT systems were delivered by December 2005. The department advised audit that the finalisation and implementation of E*Brief is the responsibility of Victoria Police, in line with a decision by the CJEP Steering Committee in mid-2007.

Regardless of who is now responsible for completing E*Brief, it is clear that E*Brief was part of the approved and funded scope of CJEP. On that basis the approved and funded scope of the CJEP program had not been fully implemented at the time of the finalisation of this report.

There have been substantial cost overruns on CJEP. The department spent $39.9 million on CJEP's development and implementation to May 2008 and Victoria Police estimates that a further $4 million will be required to complete the E*Brief project.

The initial budget for CJEP of $14.5 million was increased by $15.4 million to reflect approved scope changes to the program between 2000 and the end of 2002. In addition to funding approved by government for scope changes to CJEP since 1998, the department has supplemented CJEP's funding from its own budget on an ongoing basis.

Some of the additional expenditure on CJEP is attributable to approved scope changes to the program. These scope changes were required either to enable CJEP systems to be implemented and operated as originally envisaged—and as such, should have been identified and costed as part of the original planning and budgeting for the project—or, to provide increased functionality for agencies using CJEP systems.

The department has not recorded or monitored expenditure by CJEP partner agencies on its development and ongoing support. Advice from these agencies indicates that they have incurred around $10.4 million for costs associated with CJEP, over and above what has been spent by the department.

The department spent $18 million on maintenance, support and enhancements to the implemented CJEP systems to April 2008.

Delays in completing CJEP and the associated cost increases are mainly due to:

- underestimation of the complexity, magnitude and level of cross agency involvement required of such a project
- an inadequately developed business case that contributed to poor scoping of the project and a failure to identify realistic funding requirements
- inadequate specification of system requirements
- development and implementation issues and related delays associated with contractor performance
- fluctuating levels of commitment to and ownership of CJEP by partner agencies.

CJEP's success was highly dependent on adequate IT infrastructure being in place in partner agencies. The initial project budget made minimal provision to address infrastructure deficiencies which were evident at the program's outset. Considerably more effort could have been put into early planning for infrastructure development. The failure to do this contributed to implementation problems and delays that damaged the confidence of partner agency staff in CJEP.

1.3 Benefits realisation

The department and CJEP partner agencies advise that the implementation of CJEP has resulted in considerable benefits including:

- establishing secure links for the transmission of data between the criminal justice agencies and a middleware layer, known as the Justice Knowledge Exchange (JKE), which allows system-to-system real time transactions to be completed. The various CJEP systems—E*Justice, Case List Management System (CLMS) and the JKE—are now an integral part of the operations of the criminal justice system
- implementation of the CLMS in the County Court significantly improved the Court's capacity to manage cases from initiation to conclusion and enabled the Court to retrieve information electronically including Court outcomes
- approximately 24 per cent of all civil documents are now lodged electronically with the County Court, eliminating significant effort for court users in delivering hard copy documents to the Court
- the replacement of attendance books in police stations with an electronic record of all 'attendances at police stations' has eliminated the need for attendance book entries to be transcribed into the Law Enforcement Assistance Program (LEAP) database as this function is now performed automatically by the JKE
- the E*Justice police cell custody and property modules enable Victoria Police to share custody and property information with Corrections Victoria. The sharing of this information has eliminated the potential for confusion about risk ratings of prisoners as they move between police cells and prisons and has standardised a means of describing prisoners' property

- the immediate receipt by Victoria Police of electronic orders from both the County and Magistrates' Courts
- benefits associated with the community corrections module of E*Justice such as the electronic forwarding of an alert to the relevant case officer concerning any interaction that an offender may have had with the criminal justice system. These alerts occur in real time and are an invaluable means of community corrections officers being able to quickly gain knowledge of an offender's activities rather than having to wait for a range of administrative processes
- the automated calculation of prisoner sentences, electronic receipt of prisoner warrants, effective file tracking and property management system and automated muster counting functions in the corrections environment.

The department advised that in addition to these tangible benefits there are a range of collaborative work practice related benefits that have emerged from the program. By bringing together staff from the various criminal justice agencies to focus on business processes, CJEP has engendered a spirit of co-operation between these agencies that has not always been present in the past.

The extent of benefits delivered by CJEP has not been systematically measured, tracked and reported. While the department established a benefits capture framework early in CJEP's development it lacks a comprehensive range of performance indicators to adequately measure the benefits flowing from CJEP's implementation. In particular, performance indicators relating to intangible benefits such as better risk management of offenders, information sharing and community savings are not sufficiently robust.

There has not been regular reporting against the benefits capture framework. The lack of progressive identification, monitoring and reporting of benefits is compounded by the failure to conduct a detailed impact study to assess whether CJEP has delivered the benefits and savings projected at its inception.

The lack of systematic measurement and reporting of CJEP benefits represents a lack of accountability to ministers, stakeholders and the community, given the importance of CJEP and the extent of public funds invested in its development.

1.4 Program governance

The department has demonstrably given significant emphasis to the governance and management arrangements for CJEP since its inception and took appropriate action to strengthen CJEP's governance and management structures in response to recommendations made in our May 2003 report to Parliament on the progress of CJEP. These arrangements largely met audit's expectations.

Appropriate governance and management structures and arrangements do not, on their own, guarantee the success of a major project. There also needs to be real commitment to and ownership of the project by the stakeholders and agencies tasked with implementing it.

The CJEP Steering Committee had adequate stakeholder representation, and was provided with regular reporting by the program director regarding the program's progress. The committee was fully aware of the extent to which CJEP had exceeded its original timeframes and budget for implementation.

While high level partner agency commitment to the CJEP program was always present in a formal sense—through membership of the CJEP Steering Committee and allocation of internal resources by agencies to support the program—this was not always matched by actions and 'on the ground' commitment and ownership. It is acknowledged that the maintenance of support over long periods for major projects such as CJEP is always a challenge for participating agencies. Agencies need to balance the demands of the project with their responsibility to ensure the delivery of service obligations using available resources.

This audit identified a number of deficiencies in the application and enactment of the CJEP governance and management arrangements and in CJEP's monitoring and reporting framework, including:

- The CJEP Steering Committee did not meet often enough at a critical juncture for the project in 2002–03. This was addressed from October 2003 when monthly meetings resumed.
- Reporting to the steering committee, particularly in the earlier phase of the program's implementation lacked sufficient detail to facilitate the level of oversight and management required for such a large and complex project.
- There is no monitoring and reporting of the program's whole of project and whole of life project costs incurred by the department and other agencies.

These deficiencies adversely affected the oversight and management of CJEP's implementation and assessment of the expected program and project deliverables and outcomes.

1.5 Ongoing management and support of CJEP systems

The department needs to ensure the provision of effective ongoing support and management of CJEP systems to realise the benefits associated with its investment in the program.

The department developed and implemented an effective plan to transition the future development and support of CJEP from the primary IT contractor to the department's in-house support group. However, the decision to provide the ongoing support service for CJEP systems internally was not based on a comprehensive and fully costed business case.

The department developed a memorandum of understanding (MOU) in June 2006 to define the governance policies and arrangements for the oversight, management and coordination of the CJEP as an ongoing program. This MOU has been operational since June 2006.

1.6 Information security over CJEP

The adequacy of security over the CJEP systems and data is ultimately in the hands of the individual justice sector agencies and their staff, contractors and partners who use the systems. These agencies need to establish, maintain and adhere to effective information security management systems. There is also a need for an overarching information security policy and system governing the CJEP systems. The policies and systems of individual agencies should be consistent with the overarching requirements.

A comprehensive overarching information security policy for CJEP systems and information was established in June 2006 but it is not fully operational. Some of the actions required under that policy have not been implemented. While this matter needs to be addressed, information security policies and controls over CJEP systems are in place at the individual agency level.

The department has recognised the need for a more comprehensive approach to information security over the past two years and has taken positive steps to address weaknesses in its previous approach.

Notwithstanding this, the department needs to maintain a strong focus on ensuring that its information security management system is fully implemented and monitored for effectiveness and compliance. The department is in the process of:

- supporting the communication of the new Information Security Management System framework (ISMS) and policies to all staff, contractors and relevant partners with a coordinated training program
- completing a 'gap analysis' to identify the extent to which current practices and controls meet the requirements of the new framework and policies
- fully implementing data classification which is critical to the effectiveness of any ISMS.

1.7 Recommendations

E*Brief Project

- Victoria Police should commit to the completion of E*Brief and ensure it is delivered in line with the CJEP vision and rolled out across the police force. **(Recommendation 3.1)**
- The CJEP Governance Board should resume governance responsibility for the completion of the E*Brief project to better assure the integrity of the complete CJEP. **(Recommendation 3.2)**

Monitoring of CJEP performance and benefits

- The department should establish performance measures of a strategic nature that are linked to CJEP's expected outcomes and report performance against baseline data for these measures to both CJEP stakeholders and the Parliament through its annual report. **(Recommendation 4.1)**

Ongoing management and support of CJEP

The department needs to:

- obtain sign off to the MOU by Victoria Legal Aid to formalise the governance arrangements in place relating to CJEP
- develop a comprehensive and fully costed business case including an option analysis to justify funding levels and whether the CJEP support service should be retained internally or be outsourced
- develop and maintain a risk management strategy and risk plans to identify, manage and monitor any ongoing risks relating to CJEP systems. **(Recommendation 6.1)**

Information security over CJEP

The CJEP Information Security and Privacy Committee should commence regular annual reporting to the CJEP Governance Board on any breaches of policy or any other issues that may affect CJEP systems. **(Recommendation 7.1)**

The department should:

- ensure that the information privacy statements of CJEP partner organisations comply with the requirements of the CJEP Information Security Policy **(Recommendation 7.2)**
- establish a business continuity plan for the shared domain elements of CJEP systems **(Recommendation 7.3)**
- ensure that its data classification scheme is fully implemented and supported with appropriate guidance material as soon as possible **(Recommendation 7.4)**
- establish performance measures for the management of information security and ensure that subsequent performance is monitored and reported to senior management **(Recommendation 7.5)**
- finalise the development of an overall IT security plan that covers the building of awareness, establishes clear standards based on its Information Security Policy and ICT security policy, and defines monitoring and enforcement processes **(Recommendation 7.6)**
- establish a single configuration management database as soon as possible. **(Recommendation 7.7)**

RESPONSE provided by Acting Secretary Department of Justice

The Department would like to acknowledge the lengthy discussions that have taken place between officers of our respective organisations in an attempt to confirm the factual information in the report and to clarify matters of interpretation. The opportunity for the Secretary, DOJ to meet with you and your senior staff was also appreciated.

The Department agrees with the report's recommendations except in the two areas outlined below.

The report recommends that the CJEP Governance Board should resume governance responsibility for completion of the E*Brief Project

*The E*Brief project is part of a larger project within Victoria Police aimed at improving brief creation and management processes. The Department is satisfied that the governance and management arrangements that Victoria Police has established for this project are effective. Arrangements are also in place for the Victoria Police Deputy Commissioner with responsibility for the project to report on progress to the CJEP Governance Board.*

The report recommends that a business case be developed to justify continuation of internal support for CJEP systems

The CJEP Governance Board decided early in 2005 to establish a unit within DOJ to provide ongoing support maintenance and enhancements of CJEP systems. This decision was based on a presentation to the Steering Committee from the CJEP Project Director which examined the relative costs of outsourcing this function and establishing an internal unit. The projected costs for external provision of these services were based on experience with the then incumbent service provider. Apart from relative costs, the Steering Committee also took account of the desirability of providing an internal service support group which could become familiar with the business processes of the CJEP partner organisations and thus better understand future requirements.

The Department is satisfied that the internal unit is both effective and competitive, in cost terms, with the external market. The internal unit has been operating effectively since December 2005 and has received many compliments from partner organisations as to its responsiveness and effectiveness.

The Department also notes that the annual cost of the internal unit is at the lower end of the industry standard range for provision of maintenance and support services for complex IT systems such as CJEP.

The report contains a number of conclusions with which the Department fundamentally disagrees. While the Department acknowledges that these conclusions are audit opinion, it does not believe that they are supported by the facts.

FURTHER comment by the Auditor-General

The department's response to specific audit conclusions with which it disagrees is set out in Appendix A to this report. Rather than demonstrating that the relevant audit conclusions are not supported by the facts, this response merely presents the department's perspective on these matters.

Audit conclusions are formed following objective analysis of the evidence using criteria and considering context. This is done in accordance with audit methodology and Australian auditing standards.

RESPONSE provided by Chief Commissioner, Victoria Police

Victoria Police does not accept that a high level commitment has not always been backed up by effective action. Victoria Police's commitment to the CJEP project has been exemplified by its piloting of modules of the system over lengthy periods of time and by its preparedness to commit additional resources to the project, including people with the requisite skills. Victoria Police was not prepared, however, to introduce a system into the operational environment while significant deficiencies remained.

CJEP was an ambitious and complex IT change process. Many factors contributed to either partial success or failure. Some issues of process and acceptability of use of electronic formats still remain in the chain of users or potential users of a fully integrated criminal justice system, some of whom are not within Victoria Police.

Victoria Police remains committed to a fit for purpose electronic brief and is prepared to participate in an interdepartmental steering committee reformed to ensure the success of CJEP.

2 Background

2.1 Overview of CJEP

The Criminal Justice Enhancement Program (CJEP) is a highly complex major information technology project of the Department of Justice (the department) which commenced in January 1999.

It is an integrated Information and Communication Technology (ICT) platform designed to support the participation of the key law enforcement agencies engaged in the administration of criminal justice within Victoria including Victoria Police, the Office of Public Prosecutions (OPP), Victoria Legal Aid, the County Court and Corrections Victoria.

CJEP is designed to integrate and streamline systems and processes across agencies to minimise transaction costs and to improve access, quality and timeliness of information to agencies, courts, legal practitioners and the public.

2.1.1 Origins of CJEP

CJEP emanated from a review of administrative processes supporting the Victorian criminal justice system which commenced in 1995. The final report to government on that review, *Project Pathfinder Report—Reengineering the Criminal Justice System* (the Pathfinder report), was finalised in 1998. It recommended significant reforms to administrative practices and procedures supporting the criminal justice system at an estimated cost of $27 million over 3.5 years.

A key principle, outlined in the Pathfinder report, and underpinning the vision for an improved criminal justice system information environment, was that information should be captured once and then made accessible to authorised participants when and where needed.

Following adoption of the Pathfinder report by the government in September 1998, the department began to implement the report's major recommendations. Due to budget constraints, the department decided to implement a limited set of what were considered high priority and high impact projects which could be funded at an estimated cost of $14.5 million. Funding approval was obtained in October 1998 for implementation of these projects, which were re-badged as CJEP, with a target project completion date of November 2000.

2.1.2 Objectives and scope of CJEP

The primary objective of CJEP was to improve the recording and management of information about persons accused of criminal activity, and the disposition of criminal cases in the courts.

The program scope originally comprised the following five principal projects:

- **Accused Management Project—**involving the creation of a computer application for accessing and updating information about accused persons and their lifecycle contact with the justice system.
- **Electronic Brief/Disclosure (E*Brief) Project—**intended to improve case preparation through streamlined briefs, progressive disclosure and an early involvement process for accused persons' legal counsel.
- **Caseflow Improvement Project—**seeking improved case flow in the Magistrates' Court through integrated diversion programs and better case listing practices.
- **Case and List Management System (CLMS) Project—**involving the development of a case listing and management system in the County Court to support more active judicial supervision of criminal cases.
- **Justice Knowledge Exchange (JKE) Project**—involving the establishment of a technology infrastructure to support secure information exchange across the justice portfolio between legacy systems and new systems in each project area.

Subsequently, three projects were added to the program's scope:

- **Civil Case Management and Electronic Filing Project** (August 2000)—involving the addition of a module for civil cases to the CLMS at the County Court.
- **IT Infrastructure Development Project** (July 2001)—replacement and enhancement of the IT infrastructure—mainly at Victoria Police, but also at the department and the OPP—to facilitate the introduction of the new applications and achieve integration with partner agency legacy systems.
- **Replacement of Correction's Legacy Systems Project** (September 2002)—involving the extension of CJEP to replace significant components of three legacy systems in Corrections Victoria used for the management of offenders, the Prisoner Information Management System (PIMS), the Offender Automated Search and Information System (OASIS) and WorkMatch.

CJEP's desired end products involve computer application systems in relevant agencies working together to provide end-to-end support for criminal justice processes; from arrest and initiation of proceedings by Victoria Police, through to judgement by the courts and interaction with the corrections system in both prison and community-based corrections environments.

To this end, all of the CJEP projects outlined above have been incorporated into the following three key integrated IT software applications:

- **E*Justice—**to be used by police, prosecutions, corrections and legal aid officers, with a focus on managing information about accused persons and handling briefs of evidence.
- **ACS Courts—**to be used by the County and Magistrates' Courts with a focus on improving case management and sentencing information.
- **Justice Knowledge Exchange—**to manage the exchange of selected data between E*Justice, ACS Courts, and the legacy IT systems that remain in operation in justice agencies.

The CJEP systems are referred to collectively as the Integrated Justice Systems suite of applications or the Integrated Justice Systems (IJS). The CJEP systems operate in conjunction with a large number of legacy systems and reside in a complex set of networks in Victoria Police and the Department of Justice. IJS also includes secure links between Department of Justice, Victoria Police, Office of Public Prosecutions, Corrections Victoria and private prison providers to enable the sharing of information.

Governance arrangements

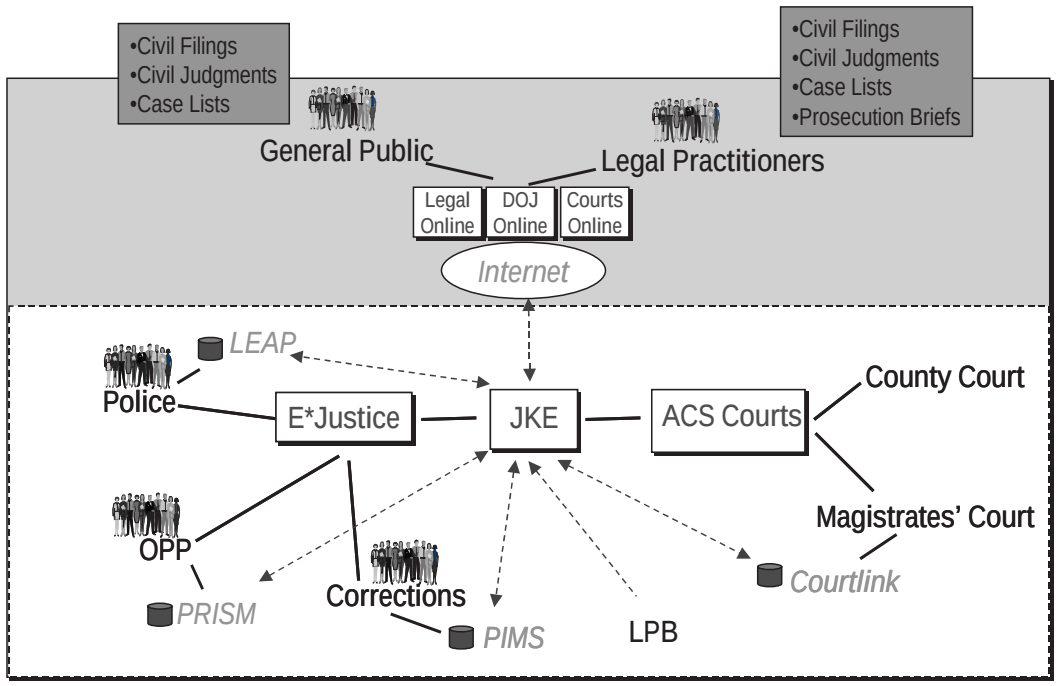
The Secretary of the department is the CJEP project sponsor and responsibility for day to day project management of CJEP has rested with the department. Implementation of CJEP has been overseen by a steering committee comprising representatives from the key agencies involved in the CJEP system and process integration project.

The department appointed a primary IT contractor in November 2000 to scope, design, build, install and support CJEP applications until June 2003. The term of this contract was extended and eventually concluded in December 2005. At that time, a unit was established within the department’s Technology Services Group to maintain, support and enhance CJEP applications into the future.

The intention was for CJEP to be accompanied by the staged delivery of a program of major cultural change across multiple agencies within the Victorian justice portfolio combining process redesign with the development of major new IT systems, people and policy related changes.

Figure 2A provides a ‘bird’s eye’ view of CJEP.

Figure 2A
CJEP—A bird's eye view



Source: Department of Justice

2.1.3 Benefits expected from CJEP

Since its inception, key benefits expected to flow from CJEP for participating agencies and the community included:

- better risk management of accused persons while in custody
- early representation for accused persons
- speedy access to the brief for the defence
- less time and effort consumed in the preparation and disposition of cases
- fewer court adjournments
- less waiting time for court users
- streamlined handling of information
- around 180 000 hours in time saved by the community each year through earlier Magistrates' Court hearings
- a 12 per cent reduction in case backlog in the County Court
- 350 000 hours in productivity gains each year by key agencies.

2.2 Audit objective and scope

2.2.1 Results of our 2003 audit

In May 2003 we reported to Parliament on the progress of CJEP and the adequacy of its management at that time. That audit did not examine the functionality of the various systems forming part of the program or the extent to which the future benefits of the project were likely to be realised.

The following key matters were raised in our 2003 report:

- While the program was initially planned to be completed by November 2000, widening of the program scope had, by then, resulted in a revised target completion date of March 2004.
- While funding of $14.5 million was initially approved for the program, scope changes resulted in the level of approved funding increasing by $20.5 million to $35 million. The additional funding mainly related to the need for an IT infrastructure upgrade; replacement of Corrections Victoria legacy systems; inclusion of a civil module in the Case and List Management System Project at the County Court; unplanned agency requests; and departmental program management costs.
- Work under a contract variation commenced in advance of appropriate approval being obtained from the department's accredited purchasing unit.

The key recommendations made in our 2003 report were for the department to:

- establish firm milestones for all remaining critical tasks to ensure close monitoring of performance against its revised March 2004 completion timeline and achievement of that timeline
- determine, monitor and report on program-wide expenditure (including the costs incurred by participating agencies) so that the aggregate program costs could be included in the department's annual report to Parliament
- ensure that the program director did not fulfil both the roles of program manager and chairperson of the program steering committee, which are incompatible
- ensure that key aspects of the program (including performance monitoring, budgetary control, risk management and quality assurance) were subject to periodic independent scrutiny by an independent body, such as the department's audit committee
- establish program performance measures of a strategic nature, linked to the program's expected outcomes
- establish ongoing support arrangements for the program beyond June 2003, when the primary IT contractor's contract expired.

2.2.2 Objective of this audit

The overall objective of this audit was to assess whether the implementation of CJEP was well managed.

To achieve this overall objective, the audit examined whether:

- CJEP has been delivered and implemented on time; on budget; and consistent with planned expectations (benefits, savings and functionality)
- appropriate governance, project management and control structures were in place to oversight and effectively manage CJEP delivery and implementation
- appropriate monitoring and reporting frameworks were in place to assess whether the expected program and project deliverables and outcomes (benefits) have been achieved
- CJEP systems and data are secure, with information security and privacy arrangements consistent with relevant legislative requirements
- appropriate structures and processes are in place for the ongoing management and support of CJEP systems.

Audit approach

This audit followed up on issues raised in our May 2003 report to Parliament on the management and progress of CJEP, focusing on the management and delivery CJEP in the four years since the previous audit. It also examined the early stages of CJEP's planning and implementation to clarify a range of issues.

The audit was performed in accordance with Australian auditing standards.

The total cost of this audit, including the preparation and printing of this report, was $385 000.

3 Implementation of CJEP

At a glance

Background

In October 1998 the Department of Justice (the department) was given approval to implement the Criminal Justice Enhancement Program (CJEP). Funding approved for the project was $14.5 million and its target completion date was November 2000.

Key findings

- CJEP is not complete and has not been implemented on time or on budget.
- Four of the five CJEP projects have been delivered but the electronic brief/disclosure project (E*Brief) may not be fully implemented until 2009.
- There have been substantial cost overruns on CJEP. The department spent $39.9 million on CJEP's development and implementation to May 2008. Victoria Police estimates that a further $4 million will be required to complete the E*Brief project.
- The initial budget for CJEP of $14.5 million was increased by $15.4 million to reflect approved scope changes to the program between 2000 and the end of 2002. In addition to funding approved for scope changes to CJEP since 1998, the department has supplemented CJEP's funding from its own budget on an ongoing basis.
- The original budget for CJEP included $1.4 million per year for expenditure on the maintenance and support of CJEP systems. This amount has subsequently been revised upwards to $6.4 million per year.
- The department spent $18 million on maintenance, support and enhancements to the implemented CJEP systems to April 2008.
- The department has not recorded or monitored expenditure by CJEP partner agencies on its development and ongoing support. Advice from these agencies indicates that they have incurred around $10.4 million for costs associated with CJEP, over and above what has been spent by the department.

At a glance – *continued*

Key findings – *continued*

- Delays in completing CJEP and associated cost overruns are mainly due to:
  - underestimation of its complexity, magnitude, and the levels of cross-agency involvement required
  - an inadequately developed business case that contributed to poor scoping of the project and a failure to identify realistic funding requirements
  - inadequate specification of system requirements
  - development and implementation issues and related delays associated with contractor performance
  - fluctuating levels of commitment to and ownership of CJEP by partner agencies.

Recommendations

- Victoria Police should commit to the completion of E*Brief and ensure it is delivered in line with the CJEP vision and rolled out across the police force. **(Recommendation 3.1)**
- The CJEP Governance Board should resume governance responsibility for the completion of the E*Brief project to better assure the integrity of the complete CJEP. **(Recommendation 3.2)**

3.1 Achievement against planned timeframes

As at May 2008, the implementation of CJEP was not complete. While four of the five projects comprising CJEP have been delivered, E*Brief, a major module of the Electronic Brief/Disclosure project, is not operating and may not be fully implemented until 2009. E*Brief is a critical component of the CJEP project. The objectives, anticipated functionality and benefits of CJEP cannot be fully realised until E*Brief is operational.

The department considers CJEP to be complete because in its view CJEP's core IT systems were delivered by December 2005. The department advised audit that it regards the finalisation and implementation of E*Brief to be the responsibility of Victoria Police, in line with a decision by the CJEP Steering Committee in mid-2007.

Regardless of who is now responsible for completing E*Brief, it is clear that E*Brief was part of the approved and funded scope of CJEP. On that basis, the approved and funded scope of the CJEP program had not been fully implemented at the time of the finalisation of this report.

Of the four core CJEP projects completed and implemented, none were completed on time. The target completion date for the overall CJEP project has been revised, at a number of key stages of the project, from November 2000 to December 2002, to March 2004 and then to February 2005, partly as a result of approved scope changes to the project. The revised target completion dates of March 2004 and February 2005 were set based on the final scope of the project but could not be met by the department.

Figure 3A illustrates the original, revised and actual completion dates for each of the CJEP projects.

Figure 3A
CJEP target completion dates and actual completion dates by project

CJEP project	Original target completion date	Revised target completion dates	Actual completion date
Electronic Brief/Disclosure	November 2000	December 2002 March 2004 February 2005	Incomplete as at May 2008 (a)
Accused Management	November 2000	December 2002 March 2004 February 2005	Progressive completion between June 2004 and December 2005
Case Improvement (Magistrates Court)	November 2000	May 2002	June 2002
Case and List Management (County Court)	November 2000	January 2002 June 2004	Progressive completion between January 2002 and December 2005
Justice Knowledge Exchange	November 2000	December 2002	May 2002

Note: (a): E*Brief is not operational. The department advised that the database and messaging capability of E*Brief have been developed and that Victoria Police is redeveloping the E*Brief user interface. The module of the Electronic Brief/Disclosure system developed for Victoria Legal Aid is not operational because of its dependency on the completion of E*Brief by Victoria Police.
Source: Department of Justice.

One of CJEP's core projects, the Case and List Management System (CLMS), which was budgeted to cost $2.9 million and has been in use since early 2002, is to be replaced during 2009 as part of the new Integrated Courts Management System (ICMS) at an estimated cost of $45 million over a four year period. This was communicated in the Attorney-General's Justice Statement *New Directions for the Victorian Justice System 2004–2014,* released in May 2004.

The development of the ICMS commenced in 2005–06. It is anticipated the ICMS will complement CJEP by providing a single cross jurisdictional case management system, and implementing a single, integrated technology platform and set of computer applications for all Victorian Courts and Tribunals.

Status of the E*Brief project

E*Brief is shorthand for electronic brief and its development was part of the original CJEP scope. The CJEP Electronic Brief/Progressive Disclosure project was designed to streamline the production and dissemination of brief documents, to facilitate pre-court communication between parties, and to encourage accused persons to seek legal advice and representation earlier in the process. The E*Brief module has several functions but is primarily intended to be a mechanism by which brief documents can be electronically prepared, authorised and disclosed to other agencies and parties in the criminal justice system.

As at May 2008, E*Brief was not operating. The department informed us that in July 2007 the CJEP Steering Committee was advised by representatives on the steering committee from Victoria Police that they did not believe it was viable to persevere with the E*Brief module because the system's user interface did not meet current Victoria Police standards. Victoria Police proposed to the committee that they would develop their own front-end or user interface for the electronic brief system and that this system would interface fully with the E-Justice database within CJEP.

The department advised that, based on this advice from Victoria Police, the CJEP Steering Committee determined that it would no longer be responsible as the governance body to deliver the Victoria Police E*Brief module. Rather, it would be a stakeholder in this exercise to ensure that the system developed by Victoria Police would effectively interface with the CJEP systems (primarily the E-Justice database) to provide electronic brief information to the other criminal justice agencies.

In effect, the CJEP Steering Committee decided to transfer responsibility for the governance and funding of the E*Brief re-development works to Victoria Police. E*Brief is central to the achievement of CJEP's objectives and the realisation of its benefits. There is risk associated with the CJEP Steering Committee's decision to step aside from its governance responsibility to complete E*Brief because, to date, Victoria Police have not delivered the E*Brief project.

The department advised that the CJEP Steering Committee is satisfied that the governance and project management arrangements in place in Victoria Police are appropriate for the delivery of the E*Brief user interface.

There have been three attempts to complete the development and implementation of E*Brief.

The first version of E*Brief was developed by the department's primary IT contractor for CJEP by around mid-2002. The system was consistent with the original system requirements that were accepted by Victoria Police in December 2000. It was piloted at three suburban police stations over 2002–2003. This version of E*Brief was not adopted by Victoria Police because:

- the system was not user friendly and there were substantial delays in printing briefs
- significant performance related issues associated with the supporting ICT infrastructure were revealed that decreased the confidence of users in the system
- there were interface difficulties with legacy systems.

As a consequence of these issues and their impact on the users' confidence in the system, Victoria Police proposed to the CJEP Steering Committee in early 2004 that the E*Brief module be redesigned to better meet the requirements of Victoria Police. This was agreed and the re-design of the E*Brief module remained part of the CJEP program with governance provided by the CJEP Steering Committee.

The second version of E*Brief was developed over the period October 2004 to March 2005 by the primary IT contractor under the stewardship of a senior project officer employed by Victoria Police and consistent with Victoria Police's revised system requirements. The revised E*Brief went into user acceptance and usability testing in Victoria Police in November 2005 and a proof of concept (POC) of the module was commenced at one police station in December 2005. This POC was followed by an extension into a second police station and was monitored by Victoria Police's central IT group.

Victoria Police advised that user testing of the second version of E*Brief revealed:

- that a large number of defects identified in version one of E*Brief were still present
- the need to review current work practices within Victoria Police to better align them with E*Brief
- presentation issues that contributed to a lack of acceptance of the system by police members.

E*Brief was further developed in October 2006 after the department's Integrated Justice Systems (IJS) unit acted on a number of change requests to rectify outstanding defects in the software and address functionality issues that emerged during the trial of the second version. However, user testing of the revised E*Brief by Victoria Police between October 2006 and March 2007 revealed:

- numerous software issues, a number of which were considered critical
- problems with the accuracy of crime statistics within Victoria Police's Law Enforcement Assistance Program (LEAP) database associated with briefs entered during the user testing due to a misalignment of then current work practices and E*Brief
- usability issues relating to the presentation layer, or front end, of E*Brief continued to undermine acceptance of the system by police members.

A status report provided by Victoria Police to the CJEP Steering Committee on 4 July 2007 advised that agreement had been reached with the department that the E*Brief front-end or 'presentation layer' will not to be used for the preparation, authorisation or disclosure of police briefs and that, in its place, a new electronic brief project had commenced. Victoria Police advised the steering committee that the re-development of the front end of E*Brief was to include:

- the alignment of brief work practices within Victoria Police to support an accelerated justice process to reduce the duration between the time of arrest and the availability of a brief of evidence
- changes to the external justice environment made in collaboration with stakeholders, including changes to legislation and policies, to support a more efficient resolution of court cases
- implementation of an electronic brief system that meets the usability requirements of operational police members and the data sharing requirements of the justice community. The back end of the E*Justice brief module would still be used to store and distribute briefs electronically.

In July 2007 we were advised by Victoria Police that the outcomes of a review of work practices associated with the development of briefs would be integral to the development of a business case for E*Brief and that the re-development of E*Brief's front end would cost around $4 million and would be funded by Victoria Police with an anticipated completion date of late 2008.

The latest advice from Victoria Police indicates that the business case will be submitted to Victoria Police command for funding consideration in the second half of 2008. On this basis, E*Brief is unlikely to be fully operational across Victoria Police until 2009. The current work by Victoria Police constitutes a third attempt to complete the development and implementation of E*Brief.

In audit's view, the following factors have contributed to the delayed implementation of E*Brief in Victoria Police:

- inadequate identification of system requirements at the outset of the project
- inadequate IT infrastructure supporting the initial version of E*Brief
- inconsistencies between existing work practices and E*Brief and a failure to identify and address this as a critical issue early in the development process
- poor performance by the primary IT contractor in the development, testing and support of E*Brief
- ineffective quality management processes exercised by Victoria Police and the department over the development and revisions of E*Brief.

These factors have both contributed to and been exacerbated by the failure of senior management of Victoria Police to achieve successful completion of the E*Brief project over the lifecycle of its development since 2001. This lack of achievement is evidenced by ongoing changes in internal responsibility for supervising and delivering the project and the fact that, at a critical stage in E*Brief's development, changes in senior command at Victoria Police left CJEP without an operational executive for over one year. This inevitably led to fluctuating momentum on the E*Brief project. At various stages the CJEP Steering Committee raised questions about the commitment of Victoria Police to the project but the committee seemed incapable of resolving this issue.

In short, while Victoria Police have maintained representation on the CJEP Steering Committee, this 'high level' commitment has not always been backed up by effective action. Notwithstanding this, it is acknowledged that the early and ongoing problems with the stability, reliability and user friendliness of E*Brief must have damaged the confidence of both police members and senior management in the system and its ability to deliver claimed benefits.

If E*Brief is not delivered in line with the CJEP vision then CJEP will have failed to achieve its objectives and many of its claimed benefits will not be realised. On this basis the CJEP Governance Board should retain accountability for oversighting the successful completion of E*Brief.

Recommendations

3.1 Victoria Police should commit to the completion of E*Brief and ensure it is delivered in line with the CJEP vision and rolled out across the police force.

3.2 The CJEP Governance Board should resume governance responsibility for the completion of the E*Brief project to better assure the integrity of the complete CJEP.

3.2 Achievement against budget

In October 1998 funding of $14.5 million was approved by government for the development, implementation and ongoing operation of CJEP over a period of 2.5 years.

Between 2000 and the end of 2002 further funding of $15.4 million was approved for scope changes to CJEP. In addition to funding approved by government for scope changes to CJEP since 1998, the department has supplemented CJEP's funding from its own budget on an ongoing basis.

Up until May 2008 the department had expended $39.9 million in CJEP development costs. As previously indicated, Victoria Police advised that further costs of around $4 million will be incurred for the re-development of E*Brief's front-end user interface. If this eventuates, the total CJEP development costs would be at least $44 million.

The CJEP partner agencies advised audit that they have incurred around $10.4 million for CJEP's development and ongoing support costs. These costs are not included in expenditure reported by the department because it has not recorded or monitored expenditure by CJEP partner agencies on CJEP's development and ongoing support.

The department spent $18 million on maintenance, support and enhancements to the implemented CJEP systems to April 2008.

The primary area where costs have exceeded the original budget is development costs. The additional development costs largely reflect approved scope changes to CJEP and an initial underestimation of the costs of developing and acquiring software and hardware associated with the CJEP systems and projects. Other development cost increases relate to extensions to the IT contract due to CJEP's expanded scope and delayed implementation.

A significant component of the development costs associated with CJEP relate to payments made to a primary IT contractor who was appointed in November 2000, following a tender process, for a term of three years with a contract value of $17 million to:

- conduct a systems scoping and requirements analysis
- design, build and install a suite of four new business applications and associated technology infrastructure to facilitate information exchange and best practice work processes throughout the Criminal Justice System

- provide 'best of breed' software including E*Justice and ACS Courts, and develop the JKE
- provide ongoing maintenance and support of the new applications up until 30 June 2003.

This contract was described as a ‘fixed price’ contract when the Attorney-General’s approval was sought for its execution. Once the contract was signed, the contractor could not make claims for additional payments based on increases in its labour costs, materials costs or inflation and exchange rate impacts. However, there was risk of legitimate claims for additional payment under the contract if there were department or partner agency caused delays and scope changes or changes to agreed system requirements.

Ultimately, the primary IT contractor was paid around $27.9 million under the contract which was extended to November 2005. The contract extensions and associated contract cost increases were appropriately authorised and primarily related to approved scope changes for CJEP and the need to extend the period for contractor support of the developed systems.

3.3 Causes of delays and cost overruns

It is clear that CJEP has not been implemented in line with its original project budget and timelines. While many factors have contributed to this outcome, audit’s analysis indicates that the department underestimated the complexity and magnitude of the project, including the extent of cross-agency involvement and cooperation required to deliver CJEP.

Factors contributing to the delays and cost overruns associated with the implementation of CJEP include:

- an inadequately developed business case
- inadequate specification of system requirements
- failure to act early to upgrade IT infrastructure
- incremental funding of CJEP’s development costs
- development and implementation issues associated with contractor performance
- fluctuating commitment to and ownership of CJEP by partner agencies, principally Victoria Police
- staff turnover and changes to the operating environment due to CJEP’s prolonged implementation
- underestimation of CJEP’s ongoing costs.

3.3.1 Inadequately developed business case

A critical component in the development of any project requiring a significant commitment of government funds is a comprehensive business case to support informed decision making on the project.

A business case should typically include the following:

- an explanation of the project objectives and how they align with the government's strategic aims
- the scope and cost of options to achieve the objectives
- an analysis of the options, including assessment of impacts and benefits
- the identification and analysis of risks for each option
- a comparative appraisal of the options in terms of their costs, benefits and risks to provide the basis for deciding which, if any, option to pursue.

CJEP originated with the Pathfinder project in 1995 which was a review of the administrative processes supporting the Victorian criminal justice system. This project was undertaken by the department to address the need for service improvement in the criminal justice system and the following specific issues:

- incompatibility of support systems which required costly, and in some cases manual, interfaces and resulted in unnecessary duplication of data and effort
- inconsistent definitions which made it difficult and costly to share data between systems and to provide operational, management and executive information in a timely manner
- a high level of inaccuracy within the data that necessitated operational staff performing unnecessary additional work
- redundant and dated procedures which prevented services being provided in a timely and cost effective manner
- potentially unnecessary legislative constraints.

The final report on the Pathfinder project was completed in July 1998 and was adopted by the Attorney-General and the Minister for Police & Corrections in September 1998. The report recommended 16 enhancements to Victoria's criminal justice system administrative processes and procedures at an estimated cost of $27 million over 3.5 years. The estimated costs and benefits identified in the report were not based on detailed functional or technical designs.

The key principle that emerged from the Pathfinder project was that Victoria's criminal justice system should be supported by an information environment in which information is captured once and then made accessible to authorised participants when and where needed.

Due to budget constraints, the department reviewed the recommendations made in the Pathfinder report and the scope of Pathfinder's implementation was then limited to a discrete set of high priority/high impact projects that could be funded on a dollar for dollar basis between the Department of Treasury and Finance (DTF) and the Department of Justice, for a total cost of $14.5 million. This set of projects was later re-badged as CJEP.

The agreement between the department and DTF was reached on the basis of a business case completed in September 1998 by the department. Audit reviewed the original business case and concluded that it:

- was prepared prior to the conduct of any detailed functional or technical designs and as such was not based on a comprehensive specification and costing of project requirements
- did not include detailed justification for proposing a project scope that failed to address a number of key Pathfinder recommendations
- lacked some of the key elements of an effective business case including:
    - a detailed cost benefit analysis, including whole of life costs and benefits
    - identification and analysis of options and recommendation of a preferred option
    - key performance measures for both project milestones and outputs
    - evidence of a commitment to re-examine and reaffirm the project objectives and the scope at each significant milestone throughout the project development process
    - identification of key risks to project delivery and a proposal for the management of these risks
    - detailed discussion of 'key related processes' to be undertaken in parallel to project implementation to facilitate effective service output delivery such as change, quality and risk management.

Given these weaknesses, the original business case was not sufficiently robust to enable an informed decision to be made on whether to proceed with the project. In addition, the business case did not contain sufficient analysis to confirm that the project scope being recommended was able to deliver the desired outcomes for around $14.5 million.

Some of the weaknesses in the original business case were addressed in revised business cases and other planning documents developed after the October 1998 decision to fund the project, including the:

- *CJEP Project Definition* (August 1999), which provided an outline of the program's management planning framework and methodology based on best practice elements from various project management methodologies including *ISO 10006: Quality management—Guidelines to quality in project management* and the Project Management Body of Knowledge method, and included the program's:
    - mission, vision, scope and key stakeholders
    - management planning framework and methodology
    - staging and key deliverables
    - governance, project, risk, change, financial and reporting management frameworks.
- *CJEP Project Risk Management Plan* (November 2000) which built on the project's definition document and set out the processes, controls and responsibilities for managing risk over the whole project including technical

development risk, contract and supplier, stakeholder, change, financial and resource management.

- revised business cases developed in May and December 2000 to support decision making on contractual arrangements for CJEP's implementation and the design phase of the program.

These documents provided the necessary framework and methodology to manage the project effectively but were completed after the planning phase of the project. In audit's view, some elements of these planning documents should have formed part of the original business case for CJEP and these documents should have been completed during the planning phase.

3.3.2 Inadequate specification of system requirements

The proper identification of system requirements is imperative to the successful development of any new IT system and requires a combination of both subject matter knowledge and IT skills.

A system requirements study (SRS) for CJEP was completed in September 2000. In December 2000, the department and the CJEP partner agencies accepted the SRS, subject to a number of qualifications that were to be addressed in the later phases of the project.

The following weaknesses in the SRS process were subsequently identified by key project participants and stakeholders:

- the SRS failed to adequately align system requirements with business processes
- partner agency staff used to identify system requirements were nominated by the partner agencies based on their substantial business knowledge or subject matter expertise and not their IT skills. While this led to the identification of functional requirements, the absence of IT skills meant that these requirements were not always successfully translated into technical requirements
- business analysts provided by the primary IT contractor to facilitate the SRS process had IT skills but limited understanding of the relevant businesses
- there was lack of clear communication between agency and IT contractor staff
- there were gaps in the functional requirements specified in the SRS, these gaps were identified by system users in the partner agencies during the user acceptance testing phase
- the SRS failed to anticipate or address critical usability issues which were subsequently raised by the users of built CJEP systems.

In September 2002 weaknesses in the initial SRS were cited by the then CJEP program director as having contributed to the need for the conduct of additional systems requirements specification work that resulted in changes to the scope of CJEP.

Critical functional gaps were identified as users progressed through each phase of detailed design review and user testing for CJEP systems and this led to unplanned development works at an additional estimated cost of at least $1 million. Had the original SRS been more effective the unplanned development works would have been minimised.

Subsequent to the original SRS being accepted by the department and all partner agencies in December 2000, Corrections Victoria performed a second SRS in late 2001, only one year after the original SRS. In addition, Victoria Police performed a further SRS for the E*Brief system in 2002, and revisited the SRS in late 2004.

3.3.3 Failure to act early on the need to upgrade IT infrastructure critical to CJEP's implementation

While the cost estimates in the 1998 Pathfinder report were based on the assumption that adequate IT infrastructure systems would be in place, the report acknowledged that this was not the case and made an assessment of the future requirements.

The department did not include costs associated with upgrading IT infrastructure in its original budget for CJEP of $14.5 million, but acknowledged that a later funding bid may be needed for infrastructure upgrade funding.

The SRS undertaken for CJEP in 2000 identified that significant IT infrastructure development would be required in order to implement the CJEP applications.

Despite the early recognition of significant IT infrastructure needs in the Pathfinder report and the obvious technological gap that a project such as CJEP would create, the development and implementation of IT infrastructure was treated as outside CJEP's original scope and was excluded from the initial project plan and budget.

Significant project delays have subsequently eventuated in relation to the necessary infrastructure upgrade not being incorporated in the initial project plan and budget.

CJEP's success is highly dependent on the adequacy of the supporting infrastructure. Considerably more effort should have been put into early planning for infrastructure development including:

- obtaining sponsor agencies' agreement on infrastructure gaps and requirements associated with the implementation of CJEP systems
- developing an overall funding strategy and budget estimation
- developing timelines for the upgrade and replacement of IT infrastructure and integrating this into the broader CJEP program implementation plans.

A consequence of the failure to act early on the need to upgrade IT infrastructure critical to CJEP's implementation was that when modules of CJEP systems were rolled out into agencies for piloting and user acceptance testing, infrastructure related problems caused stability and reliability issues that ultimately undermined the confidence of users in the systems. This was not ideal for a multi-agency ICT project that was meant to be accompanied by changes in work practices and culture.

3.3.4 Incremental funding of CJEP development costs

Determining and securing adequate funding at the outset is crucial to the success of any project. The level of funding is usually an indication of the size and complexity of the project and should inform the organisational, governance and project management structures, frameworks, and processes required to manage the project's implementation effectively.

The CJEP project experience clearly demonstrates that there was a failure to identify and secure sufficient funding to deliver the project at the outset.

Funding of $14.5 million was approved in October 1998 for the development, implementation and ongoing operation of CJEP to 30 June 2003. This funding was sourced from the Department of Treasury and Finance ($7 million) and the Department of Justice ($7.5 million). The approved original budget included $11 million for the identification of systems requirements and development and project management of CJEP. The remaining $3.5 million in the approved budget was allocated to recurrent support and maintenance costs.

Between 2000 and the end of 2002 further funding of $15.4 million was approved for scope changes to CJEP. In addition to funding approved by government for CJEP since 1998, the Department of Justice has supplemented CJEP's funding from its own budget on an ongoing basis.

As at May 2008, approved funding for CJEP's development costs totalled $39.9 million. Figure 3B shows the funding sources for these development costs.

Figure 3B
Funding sources for CJEP development costs
($ million)

	Total
Initial funding by Department of Justice (November 1998)	7.50
Initial funding by DTF (November 1998)	7.00
Funding provided subsequent to initial budget approval	
Transfer of funds from County Court Project for civil module of CLMS (April 2000)	2.90
ERC funding for IT infrastructure development (March 2001)	8.00
ERC funding for replacement of OASIS system in Corrections (September 2002)	1.10
ERC funding for replacement of PIMS system in Corrections (September 2002)	3.40
Agency contributions from existing budgets	0.25
Department supplementation since November 1998	9.74
Total	**39.89**

Source: Department of Justice.

Some of the additional funding decisions set out in Figure 3B relate to matters that were either known, or should have been known, when the original budget for CJEP was established in October 1998.

Specifically, additional funding of $8 million for a major IT infrastructure upgrade, mainly affecting Victoria Police, was required when testing of the E*Brief module in 2001 identified significant development and infrastructure performance issues. Although some infrastructure upgrades were allowed for and undertaken as part of CJEP's original scope and budget, a state-wide justice sector IT infrastructure upgrade, as recommended in the Pathfinder report in July 1998, was omitted from CJEP's original scope and budget, despite the Pathfinder report stating that such an upgrade was considered critical to the whole project.

The department was unable to provide any documented justification for this omission. However, in a document reconciling CJEP's original scope to the recommendations made in the Pathfinder report the department acknowledged that a later bid may be needed for infrastructure upgrade funding.

The omission of this significant item from the original CJEP budget indicates a lack of proper and realistic project planning. In addition, it is clear that the department should have recognised at the time the original budget for CJEP was established that it would not be sufficient to enable successful delivery of the project.

Audit considers that the funding of $4.5 million approved by ERC in September 2002 for the replacement of legacy systems in Corrections Victoria related to matters that reasonably, should have been foreseen had the CJEP project been adequately planned.

In October 2001, around one year after accepting the original SRS for CJEP, Corrections Victoria identified the need to replace certain legacy systems that either interfaced with or were parallel to CJEP systems. While the case to replace the legacy systems was linked to changes in Corrections Victoria's business environment, including changes to legislation, in our view these changes, together with the need for CJEP systems to interact with existing Corrections Victoria IT systems, could have been anticipated and included in the original SRS for CJEP.

The addition of the civil module to the CLMS for the County Court at a cost of $2.9 million was a legitimate scope variation that could not have been included in the original project budget. Originally, the scope of CJEP was to include criminal matters only. However, in April 2000, when the County Court re-assessed its business requirements and identified a need for a new case list system for civil cases, it was agreed with the department that the best option would be to add a civil cases module to the existing CLMS within CJEP's scope.

This was seen as having the advantages of avoiding additional costs associated with developing a new and separate or stand-alone system and eliminating the need for County Court users and staff having to deal with two separate case listing systems. Funding was transferred to the CJEP budget by the County Court because the responsibility for delivering the civil module of a case and list management system for the County Court was added to the CJEP scope.

The matters outlined above indicate an incremental approach to the funding of CJEP rather than the provision of a total funding package to match the real and known requirements of the program. This incremental approach resulted in fundamental requirements being omitted from CJEP's scope which, in turn, led to the selection of interim solutions until further funding became available to the department or the partner agencies.

Consequently, system requirements specification exercises were needed to be performed more than once. Scope changes were made to address these revised requirements and for matters that were known to be issues at the commencement of the CJEP program—for example, the need to upgrade IT infrastructure at Victoria Police to facilitate the implementation of CJEP projects, and the need to increase CJEP's functionality to replace existing legacy systems in partner agencies such as Corrections Victoria.

Ultimately, this piecemeal approach to the funding of CJEP has contributed to the delayed implementation of CJEP and its cost overruns.

3.3.5 Development and implementation issues associated with contractor performance

The primary responsibility for developing, testing and implementing CJEP systems rested with the primary IT contractor appointed by the department in November 2000 under a fixed price contract for $17 million, that was due to expire at the end of June 2003.

Our review of CJEP Steering Committee minutes revealed that from 2003 onwards there were concerns and issues raised by partner agencies and the department regarding the performance of the primary IT contractor. These concerns primarily related to the quality of work performed by the contractor and the quality, quantity and continuity of human resources assigned to the project tasks. The IT contractor attended steering committee meetings periodically and did acknowledge many of the issues and concerns raised.

The department commissioned a consultant to review the operation of the contract arrangements between the department and the primary IT contractor. The results of the initial review and a follow-up review were reported to the CJEP Steering Committee in February 2004 and June 2005 respectively.

These reviews focused on: assessing the level of compliance with the terms of the principal IT contract established in November 2000; evaluating the quality of products and service standards of the contractor; developing strategies for the acquisition of support services for CJEP at the expiry of the IT contract; and identifying transitioning issues from the IT contractor to the department's Integrated Justice System (IJS) unit.

The consultant's February 2004 report concluded that:

- the IT contractor had substantially complied with the terms and conditions of the contract, including the parts relating to the development, installation and integration of hardware and software
- stakeholder acceptances for all contract deliverables had been evidenced, with the exception of E*Brief and Court Order modules, where significant performance-related issues were apparent. The contractor was providing remediation or development works for these two modules to the satisfaction of the stakeholders and was therefore complying with its warranty obligations
- the quality of products and standard of services supplied by the IT contractor had not been acceptable to the stakeholders with specific deficiencies identified by stakeholders and acknowledged by the IT contractor, which recognised weaknesses within its approach to software development and systems integration, and to project management. Specific deficiencies included:
  - design documents that represented functional requirements, but possessed insufficient technical requirements
  - an inexperienced development team, relative to the nature of the task
  - project managers were too distant from day to day concerns of the project team and maintained insufficient contact with stakeholders
  - quality procedures for software development and testing were neither followed nor enforced with sufficient rigour
  - inadequate response to stakeholder feedback at the agency practitioner level.

The consultant also identified a range of factors relating to the department's management of CJEP that had contributed to difficulties and delays faced by the contractor. For example, the consultant concluded that the complexity of the consultation, specification and approvals process of the department, given its extensive number of stakeholders, contributed to delays to the progress of the project.

Ultimately, problems with the primary IT contractor's performance contributed to the cost and time overruns on CJEP's implementation. The CJEP Steering Committee periodically raised concerns with the senior management of the contractor and discussed escalating action against the contractor at various points.

3.3.6 Fluctuating commitment to and ownership of CJEP by partner agencies

Successful implementation of a complex ICT project across multiple agencies requires real commitment and ownership by the leaders of the agencies involved and that commitment needs to be backed up by the allocation of sufficient and appropriate resources and management attention to project delivery.

The maintenance of support over long periods for major projects such as CJEP is always a challenge for participating agencies. Agencies need to balance the demands of the project with their responsibility to ensure the delivery of service obligations using available resources.

As noted already, there were successive failures of senior management of Victoria Police to achieve successful completion of the E*Brief project over the lifecycle of its development since 2001.

Audit's review of CJEP Steering Committee minutes indicated that the commitment to and ownership of CJEP by Victoria Police and other partner agencies fluctuated at various stages of CJEP's development. This is evidenced by:

- questions raised by the steering committee about the level of agency executive involvement in CJEP delivery
- lack of availability of agency staff for system piloting and acceptance testing at various stages
- changes to agency staff assigned to CJEP implementation and supervision
- questions raised by partner agencies regarding quality and implementation problems and delays with CJEP systems and the impact this was having on the confidence of their staff in the project as a whole.

While all partner agencies remained represented on the committee and did allocate internal resources to assist delivery of the project, it was apparent that the commitment and ownership levels within agencies fluctuated over time and this contributed to delays in CJEP's implementation.

3.3.7 Prolonged implementation of CJEP

As indicated previously, the target project completion date for CJEP has been revised, at a number of key stages of the project, partly as a result of approved scope changes, from November 2000 to December 2002, to March 2004 and then to February 2005. These target dates were not met by the department.

While four of the five projects comprising CJEP have been delivered, E*Brief, a major module of the Electronic Brief/Disclosure project, is not operating.

CJEP was conducted as a five stage project as shown in Figure 3C below.

Figure 3C
CJEP project stages

Stage	Stage description	Proposed completion date	Actual completion date
Stage 1	Concept planning and set-up	June 1999	May 1999
Stage 2	Concept analysis and design	December 1999	December 2000
Stage 3	Development, integration and installation	June 2000	Incomplete with E*Brief not expected to be operational until 2009
Stage 4	Implementation and handover	November 2000	Incomplete with an expected completion date of 2009
Stage 5	Ongoing support	Ongoing from August 2001	N/A

Source: Victorian Auditor-General's Office.

The project remains incomplete, as the Victoria Police Electronic Brief (E*Brief) module is not expected to be fully implemented and operational until 2009. If Victoria Police achieves that timeline, the project will have taken nine years to complete.

The prolonged implementation of CJEP has, of itself, resulted in other problems and challenges which have caused further delays and cost pressures. These problems and challenges have included:

- considerable changes in technology and business processes
- changes to the criminal justice environment, including the Long-term Prisons Management Strategy and the Community Correctional Services Redevelopment Plan impacting on the way prisoners are being managed
- legislative changes relating to privacy, drug court and sentencing
- significant turnover of staff involved in CJEP's implementation, both at the department level and the partner agency level, resulting in loss of knowledge and changed perspectives regarding its implementation.

These factors have contributed to considerable unplanned but necessary modifications to the original products selected and consequential cost and time overruns on the CJEP program.

3.3.8 Underestimation of CJEP's ongoing costs

Another area where the original budget for CJEP was evidently deficient was its estimation of the annual costs required for maintenance and support of the systems once they were operating. The original budget of $14.5 million included $1.42 million per year for the maintenance and operation of the CJEP systems for a period up to 30 June 2003.

The amount required for annual maintenance and support of CJEP systems was revisited in 2003–04 by consultants appointed by the department and revised upwards to $5.6 million per annum. This amount was revised upwards again in 2005 to $6.4 million per annum, and was endorsed by the CJEP Steering Committee in May 2005.

The revised annual budget of $6.4 million covers the department's costs in providing ongoing maintenance and operation of CJEP and includes the provision of support to all partner agencies. Notwithstanding this, additional costs will be incurred at the agency level.

The costs of ongoing maintenance and support were originally covered as part of the November 2000 contract with the primary IT contractor and $3.5 million was allowed for ongoing maintenance and support in the contract price. Around $4.8 million of the $27.9 million paid to the primary IT contractor between November 2000 and December 2005 related to ongoing maintenance and support of CJEP systems.

By April 2008, $18 million had been expended on the maintenance, support and enhancement of CJEP systems. The department was not able to provide a break-up of what costs have been incurred for enhancements which may need to be capitalised.

Of the $18 million, around $11.8 million relates to the department's IJS unit, which is responsible for the ongoing maintenance, support and enhancement of CJEP. The balance of $6.1 million represents payments to the primary IT contractor and temporary contractors that performed the maintenance and support function prior to the formation of the IJS unit for a short period after the expiry of the primary IT contractor's contract in November 2005.

3.4 Overall conclusion

The delays and cost overruns experienced by the CJEP project can be attributed to the following root causes:

- inadequate planning at its inception
- failure to identify and secure funding for whole of life cycle costs (capital and recurrent) required to deliver the program at its inception
- contractor performance
- fluctuating commitment to and ownership of CJEP by partner agencies.

4 Benefits realisation

At a glance

Background

CJEP was an ambitious and complex IT change project involving the implementation of five discrete, but linked, projects designed to improve access, quality and efficiency in the criminal justice system.

Key findings

- The Department of Justice (the department) advises that CJEP is delivering considerable benefits across the criminal justice system.
- The benefits resulting from CJEP's implementation have not been systematically and rigorously measured, tracked and reported. On this basis, audit can give no assurance that these claimed benefits have been delivered.
- While the department established a benefits capture framework early in CJEP's development it lacks a comprehensive range of performance indicators to adequately measure the benefits emanating from CJEP's implementation. In particular, performance indicators relating to intangible benefits such as better risk management of offenders, information sharing and community savings are not sufficiently robust.
- There has not been regular reporting against the benefits capture framework. The lack of progressive identification, monitoring and reporting of benefits is compounded by the failure to conduct a detailed impact study to assess whether CJEP has delivered the benefits and savings projected at its inception. The lack of systematic measurement and reporting of CJEP benefits represents a lack of accountability to ministers, stakeholders and the community given the importance of CJEP and the extent of public funds invested in its development.

Recommendation

- The department should establish performance measures of a strategic nature that are linked to CJEP's expected outcomes and report performance against baseline data for these measures to both CJEP stakeholders and the Parliament through its annual report. **(Recommendation 4.1)**

4.1 CJEP's expected outcomes and benefits

The Pathfinder project report estimated that tangible productivity savings totalling around $24 million could be achieved over four years if its recommendations were fully implemented. The estimated cost of implementing all the Pathfinder project recommendations was $27.5 million over 3.5 years. The CJEP project sought to address a subset of the Pathfinder recommendations.

The underlying vision for CJEP was to develop an integrated Information and Communication Technology (ICT) platform to support the participation of the key law enforcement agencies engaged in the administration of criminal justice within Victoria, including Victoria Police, the Office of Public Prosecutions, Victoria Legal Aid (VLA), the County Court, the Magistrates' Court and Corrections Victoria.

At CJEP's inception it was anticipated that the integration of disjointed systems used across the Victorian criminal justice system and the associated move to electronic storage, handling and sharing of information would deliver a range of benefits to the community and sponsor agencies.

In 1999 the department identified a range of tangible and intangible benefits for the partner agencies, accused persons, legal practitioners and the community associated with implementation of CJEP, including:

- better risk management of accused persons while in custody
- early representation for accused persons
- speedy access to the brief for the defence
- less time and effort consumed in the preparation and disposition of cases
- fewer court adjournments
- less waiting time for court users
- streamlined handling of information
- time savings of around 180 000 hours per year for the community from earlier Magistrates' Court hearings
- a 12 per cent reduction in case backlog in the County Court
- 350 000 hours in productivity gains each year by key agencies.

These benefits were primarily attributed to the expected positive impact of CJEP on the administrative processes and systems within the criminal justice system.

The economic value of the benefits was estimated to be around $13 million annually when all process changes and systems were fully implemented. Revisions to these benefits were made in subsequent business cases supporting requests for additional funding for CJEP.

The most recent revised estimation of CJEP's benefits was undertaken in September 2003 by a consultant commissioned by the department to review CJEP's progress and assess options and funding requirements for its completion and ongoing support.

The consultant identified the potential achievement of projected full business case gross benefits of between $13.8 million and $15.2 million per year comprising:

- $0.6 million to $1.7 million in realisable partner agency savings
- $9.3 million to $9.6 million of partner agency productivity and efficiency benefits
- $3.9 million in benefits for the community and legal practitioners.

These estimated benefits do not compare favourably with the expected total development costs for CJEP of around $44 million, together with the estimated annual support costs of $6.4 million.

4.2 Realisation of outcomes and benefits

The department advised that substantial progress has been made towards the achievement of CJEP's key deliverables resulting in considerable benefits including:

- establishing secure links for the transmission of data between the criminal justice agencies and a middleware layer known as the Justice Knowledge Exchange (JKE) which allows system to system real time transactions to be completed. The various CJEP systems—E*Justice, Case List Management System (CLMS) and the JKE are now an integral part of the operations of the criminal justice system
- the availability of more current and accessible information about accused persons throughout their lifecycle of contact with the criminal justice system
- implementation of the CLMS in the County Court significantly improved the Court's capacity to manage cases from initiation to conclusion and enabled the Court to retrieve information electronically including Court outcomes
- improved caseflow in the Magistrates' Court through better case listing practices and integrated diversion programs.
- approximately 24 per cent of all civil documents are now lodged electronically with the County Court, eliminating significant effort for court users in delivering hard copy documents to the Court
- the replacement of attendance books in Police stations with an electronic record of all 'attendances at Police Stations' has eliminated the need for attendance book entries to be transcribed into the Law Enforcement Assistance Program (LEAP) database as this function is now performed automatically by the JKE
- the E*Justice Police cell custody and property modules enable Victoria Police to share custody and property information with Corrections. The sharing of this information has eliminated the potential for confusion about risk ratings of prisoners as they move between police cells and prisons and has standardised a means of describing prisoners' property
- the immediate receipt by Victoria Police of electronic orders from both the County and Magistrates' Courts

- benefits associated with the community corrections module of E*Justice such as the electronic forwarding of an alert to the relevant case officer concerning any interaction that an offender may have had with the Criminal Justice system. These alerts occur in real time and are an invaluable means of community corrections officers being able to quickly gain knowledge of an offenders activities rather than having to wait for a range of administrative processes
- the automated calculation of prisoner sentences, electronic receipt of prisoner warrants, effective file tracking and property management system and automated muster counting functions in the corrections environment.

The department advised that in addition to these tangible benefits there are a range of collaborative work practice related benefits that have emerged from the program. By bringing together staff from the various criminal justice agencies to focus on business processes, CJEP has engendered a spirit of cooperation between these agencies that has not always been present in the past.

It is accepted by the department, partner agencies and consultants engaged by the department that E*Brief is crucial to the end-to-end integration of CJEP and to the full realisation of the benefits and functionality expected from CJEP's implementation.

A number of CJEP modules are dependant on the implementation of E*Brief before they can become fully operational. Yet, E*Brief is not expected to be completed until 2009. The consultant commissioned by the department in 2003 to review CJEP's progress and assess options and funding requirements for its completion concluded that failure to complete E*Brief would result in significant benefits being foregone by Corrections Victoria, Magistrates' and County Courts and the OPP.

Consequently, the delayed implementation of E*Brief has directly impacted on the:

- achievement of a key deliverable to develop an end-to-end system application for managing information about an accused person
- VLA brief module which has been developed but is not operational due to its dependency on E*Brief
- delivery of full functionality of other modules within OPP, the Magistrates' Court and Corrections.

When CJEP is fully implemented, the following outcomes or benefits are expected to be realised:

- accessing of briefs online by VLA and private defence counsel, which is expected to result in fewer hearings before case resolution because defence counsel will have earlier access to more information
- achievement of full functionality of other modules affected by E*Brief, resulting in overall productivity gains gained from a reduction in the current duplication of data entry and handling across justice agencies.

The CJEP program was also seen as having the added potential of facilitating, through its established infrastructure, implementation of future e-government initiatives in the justice portfolio.

While the department and partner agencies advise that the implementation of CJEP to-date has resulted in considerable benefits, the extent of benefits delivered has not been systematically and rigorously measured, tracked and reported. This lack of progressive identification and monitoring of benefits is compounded by the failure to conduct a detailed impact study to assess whether CJEP has delivered the benefits and savings projected at its inception. Consequently, audit is unable to provide assurance regarding what benefits or savings have been achieved or foregone from the implementation of CJEP.

Benefits capture and monitoring framework

The department established a benefits capture framework early in CJEP's development that identified the benefits anticipated from the implementation of CJEP in the following areas:

- fast, reliable information sharing between connected agencies
- productivity gains
- community time savings
- access to briefs
- more timely disposition of cases
- better risk management of offenders.

This benefits capture framework has not been fully underpinned by a robust set of qualitative and quantitative performance indicators and measures and associated baseline data that would enable progressive measurement of benefits delivered by CJEP.

Many of the performance indicators and measures established by the department for CJEP require a high degree of qualitative judgement to be exercised rather than being based on objectively measurable data. Examples of such indicators or measures include 'improved management oversight', 'productivity gains' and 'better quality data'. Performance against such measures is reported in percentage terms rather than on the basis of clearly defined and verifiable data items.

In February 2006 the CJEP Steering Committee agreed that a working party of representatives from the CJEP partner agencies should be convened to review the benefits realisation framework and recommend a comprehensive framework of measures to the committee. The department advised that a meeting convened to review the benefits framework concluded that a revision was required to reflect contemporary experience as many of the performance measures were considered to be potentially no longer relevant.

The department lacks a comprehensive range of performance indicators to adequately measure the benefits emanating from CJEP's implementation. In particular, performance indicators relating to the intangible benefits such as better risk management of offenders, information sharing and community savings are not sufficiently robust.

In addition, a number of the performance indicators would be difficult to measure and to establish a baseline against which subsequent performance could be compared. Assessing the extent to which trends in performance against these indicators are solely attributable to CJEP presents further significant challenges.

We found that the CJEP Steering Committee was presented with reports indicating progress against the benefits capture framework on only a few occasions during the development of CJEP. The department has failed to undertake systematic, regular and detailed monitoring and reporting of the benefits and savings emanating from CJEP.

The department advised that the focus has been on completing CJEP's implementation and that the task of monitoring CJEP and its benefits capture will be the responsibility of the CJEP Operational Management Committee established under CJEP's new governance structure.

Given that CJEP has been under development since 1999 and the fact that four of the five key CJEP projects have been operating for over two years, we expected that the department would have established measures of a strategic nature that are linked to the program's expected outcomes some time ago. We made a recommendation to this effect in our 2003 report to Parliament on the progress of CJEP.

The department's response to that report indicated that a series of strategic measures had been formulated and would be included in future reporting to Parliament. To date, no such reporting has occurred and there is little evidence that the department has developed a series of strategic measures linked to the program's expected outcomes.

In the absence of adequate reporting against the CJEP benefits capture framework by the department, we reviewed information publicly available from the Australian Bureau of Statistics[1] and Productivity Commission[2] to identify relevant performance indicators and data which may show trends in the efficiency of the justice and court systems in Victoria over time. This analysis did not provide any conclusive evidence of a more or less efficient justice system in Victoria over the past 3 years.

The analysis did indicate that the targeted 12 per cent reduction in case backlog in the County Court identified by the department in 1999 is unlikely to have been achieved because the pending caseload for appeals in the County Court has steadily increased from 510 cases at 30 June 2003 to 1094 cases at 30 June 2007. The pending caseload for non-appeal cases in the County Court has steadily increased from 1722 at 30 June 2003 to 2467 cases at 30 June 2007[3].

---

[1] Australian Bureau of Statistics, 2006–07 *4513.0 Criminal Courts Australia*, 25 January 2008.

[2] Productivity Commission, Report on Government Services 2008, Commonwealth of Australia 2008.

[3] Productivity Commission, Report on Government Services 2008, Commonwealth of Australia 2008.

Recommendation

4.1 The department should establish performance measures of a strategic nature that are linked to CJEP's expected outcomes and report performance against baseline data for these measures to both CJEP stakeholders and the Parliament through its annual report.

4.3 Overall conclusion

While the department and partner agencies advise that the implementation of CJEP to-date has resulted in considerable benefits, the extent of benefits delivered has not been systematically and rigorously measured, tracked and reported.

While the department established a benefits capture framework early in CJEP's development, it lacks a comprehensive range of performance indicators to adequately measure the benefits emanating from CJEP's implementation. In particular, performance indicators relating to intangible benefits such as better risk management of offenders, information sharing and community savings are not sufficiently robust.

There has not been regular reporting against the benefits capture framework. The lack of progressive identification, monitoring and reporting of benefits is compounded by the failure to conduct a detailed impact study to assess whether CJEP has delivered the benefits and savings projected at its inception.

The lack of systematic measurement and reporting of CJEP benefits represents a lack of accountability to ministers, stakeholders and the community given the importance of CJEP and the extent of public funds invested in its development.

In the absence of regular reporting against a robust benefits capture framework or a detailed impact study we have been unable to conclude on what benefits or savings have been achieved or foregone from the implementation of CJEP.

5 Program governance

At a glance

Background

The magnitude and complexity of CJEP required the establishment and periodic review of a well structured program governance and management framework.

Key findings

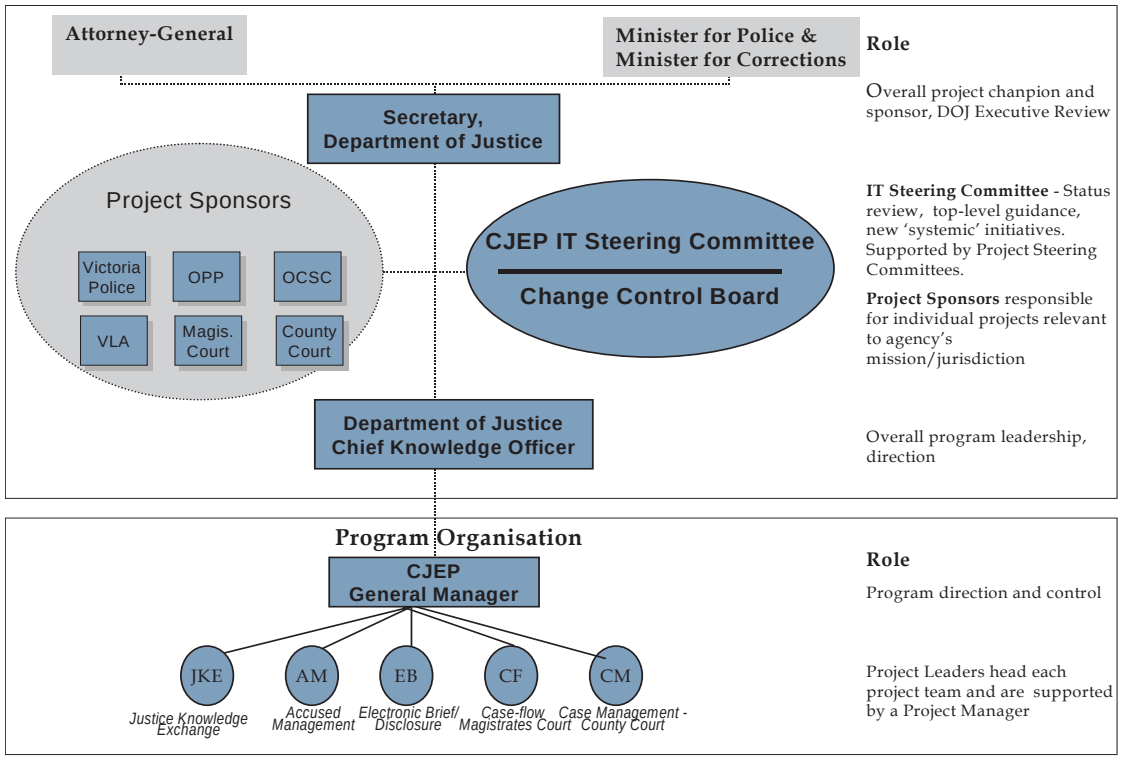
- The Department of Justice (the department) has demonstrably placed significant emphasis on the governance and management arrangements for CJEP since its inception, and these arrangements largely met audit expectations.
- The CJEP Steering Committee had adequate stakeholder representation, and was provided with regular reporting by the program director regarding the program's progress. The committee was fully aware of the extent to which CJEP had exceeded its original timeframes and budget for implementation.
- The department took appropriate action to strengthen CJEP's governance and management structures in response to recommendations made in our May 2003 report to Parliament on the progress of CJEP.
- While high level partner agency commitment to the CJEP program was always present in a formal sense through membership of the CJEP Steering Committee and allocation of internal resources by agencies to support the program, this was not always matched by actions and 'on the ground' commitment and ownership.
- We identified deficiencies in the application and enactment of the CJEP governance and management arrangements and in CJEP's monitoring and reporting framework that adversely affected the oversight and management of CJEP's implementation and assessment of the expected program and project deliverables and outcomes.

5.1 Overview of CJEP governance

CJEP's governance, management structures and processes including its risk, quality and change management plans were originally outlined in the CJEP Project Definition document which was completed in August 1999.

Figure 5A provides an overview of CJEP's governance and management structure, as established in 1999. The structure has varied slightly over the period of CJEP's implementation but remained largely intact.

Figure 5A
CJEP Governance and Management Structure



Source: Department of Justice.

The key layers of CJEP's governance and management structure were as follows:

- **Secretary of the department**—the project champion and provides project oversight in the role of chairperson of the CJEP Steering Committee
- **CJEP Steering Committee**—oversight responsibility for the delivery and governance of CJEP and includes agency project sponsors from Victoria Police, Corrections Victoria, County Court, Magistrates' Court, Victoria Legal Aid and Office of Public Prosecutions

- **Program Director**—overall project responsibility including project planning, liaison with agency project sponsors, financial, change, quality and risk management issues. Reports to the steering committee, the project champion and the relevant ministers. In February 2002, the Program Director was promoted to Chief Knowledge Officer within the Department of Justice but maintained overall responsibility for CJEP. A CJEP General Manager was appointed to perform the day to day functions previously performed by the Program Director. This was subsequently reversed in October 2003 due to change and quality management issues
- **Contract Management Group**—consisted of a contract administrator (CJEP Program Director), contract manager and contract monitor responsible for monitoring the progress of the contract to ensure that all the tasks are implemented within budget, on time, and to the satisfaction of all agencies concerned. This group reported to the CJEP steering committee through the Program Director
- **Project Teams**—led by project managers and supported by team leaders and business analysts, were initially established with cross-agency responsibility for resolving all issues specifically related to each of the five projects making up CJEP (Accused Management, Electronic Brief, Caseflow Improvement, Case and List Management System, and JKE). The project teams were periodically re-allocated to better reflect CJEP's changed implementation phases.

In addition to the above structures, the following management processes were put in place:

- **budget and financial management**—through the department's Finance Unit with regular reviews exercised by the department's Secretary, as project champion, and chief financial officer. A dedicated financial resource to the CJEP Project Team was also appointed in December 2003, with responsibility for day to day cost management and reporting
- **monitoring and reporting**—regular status reports were provided to the steering committee by the Program Director and key contractors responsible for major deliverables. The Program Director also reported to the Secretary and the relevant ministers.

5.2 Previous audit findings

Our May 2003 report to Parliament on the progress of CJEP included an assessment of the adequacy of the project's governance and management at that time. The key recommendations made in our 2003 report included that the department:

- ensure that the Program Director did not fulfil both the roles of program manager and chairperson on the program steering committee, which are incompatible
- ensure that key aspects of the program (including performance monitoring, budgetary control, risk management and quality assurance) were subject to periodic independent scrutiny by an independent body, such as the department's audit committee

- determine, monitor and report on program-wide expenditure (including the costs incurred by participating agencies) so that the aggregate program costs could be included in the department's annual report to Parliament.

Audit followed up the department's action on these recommendations and examined whether the department had established, and maintained throughout the program's lifecycle, robust program/project management and control structures including:

- comprehensive program implementation/management plans—with clearly documented delivery objectives (including anticipated benefits/savings and functionality), scope, budgeted costs and delivery timelines; together with supporting project management plans (including quality, change and risk management)
- a program steering committee to oversee and manage CJEP—with appropriate membership/representation and skills; clear roles and responsibilities; and regular meetings to facilitate effective program management and direction
- a program director with clear roles, responsibilities and accountabilities, to oversee and manage the individual project teams and regularly report to the program steering committee
- project teams for the major projects within CJEP—maintaining effective project risk management, quality management, change management and contract management practices, and timely reporting to the program director and program steering committee on project progress and performance
- a comprehensive program risk management strategy, register and management process
- effective and timely reporting of the program's implementation progress to the program director, steering committee and senior management—with appropriate and timely action taken in response to the results of any performance deviation
- the conduct of periodic independent reviews (internal or external) of program management and progress—with appropriate and timely action taken in response to any findings or recommendations made.

5.3 Effectiveness of CJEP governance

The department has demonstrably placed significant emphasis on the governance and management arrangements for CJEP since its inception and these arrangements largely met audit expectations. However, appropriate governance and management structures and arrangements do not, on their own, guarantee the success of any major project. There also needs to be real commitment to and ownership of the project by the stakeholders and agencies tasked with implementing it.

There is clear evidence that the CJEP Steering Committee had adequate stakeholder representation, and was provided with regular reporting by the program director regarding the program's progress including financial, change, quality, risk and contract management issues and further reporting by key contractors regarding their deliverables. On this basis, the steering committee was fully aware of the extent to which CJEP had exceeded its original timeframes and budget for implementation.

In addition, following recommendations made in our May 2003 report to Parliament on the progress of CJEP and the results of a review of CJEP by a consultant appointed by the department in 2003, the following changes were made to further strengthen CJEP's governance and management structures:

- the Secretary of the department replaced the Program Director as the chairperson of the CJEP Steering Committee
- steering committee meetings were held on a monthly basis from October 2003
- monthly meetings (or more frequently if required) were held in the period October 2003 to December 2005 between the chairperson of the CJEP Steering Committee, the CJEP Program Director and the responsible IT contractor to monitor progress and resolve outstanding issues
- the Chief Knowledge Officer of the department was seconded back to the full time position of CJEP Program Director in October 2003 to address issues which had arisen following his transfer from that position in February 2002.

A detailed CJEP Project Risk Management Plan was prepared by the CJEP Program Director in November 2000. This document provided a framework setting the processes, controls and responsibilities for managing risk over the whole CJEP development program.

A CJEP risk register was also developed and maintained by the Program Director with input from project managers, suppliers and stakeholder representatives who are encouraged to monitor, identify and manage risks relating to CJEP. The risk register included the most significant risks to CJEP, the ranking of the risks with the likelihood of the risk occurring and the controls or mitigation strategies to reduce the likelihood of the risk occurring. All key risks were reported by the Program Director at each CJEP Steering Committee meeting. CJEP risks were incorporated in the department's risk register.

Notwithstanding this, we identified a number of deficiencies in the application and enactment of the CJEP governance and management arrangements that have undermined the effectiveness of these arrangements, specifically:

- Both the original and revised Terms of Reference for the CJEP Steering Committee briefly state the purpose and membership of the committee but lack clear and detailed direction in respect of the purpose, objectives, roles, responsibilities and authority of the committee, its chairperson and members; and do not set out governance, communication and reporting requirements and meeting protocols.

- The CJEP Steering Committee did not meet often enough during a critical period for the project in 2002–03. This was addressed from October 2003 when monthly meetings resumed.
- The CJEP Steering Committee was provided with insufficiently detailed reporting on project progress in the period in the earlier phase of the program's implementation. In addition, between May 2003 and August 2004, the level of project progress reported to the committee fluctuated between 80 per cent and 85 per cent with little explanation for the apparent slowdown or stalling of progress.
- The target completion date for the project reported to the CJEP Steering Committee progressively moved outwards with no explicit approval of this by the committee.
- The CJEP Program Director who has overall project management responsibility was also a member of the CJEP Steering Committee, potentially affecting the level of independent scrutiny by the committee.
- The transfer of the CJEP Program Director from the day to day management of CJEP in the period February 2002 to October 2003, a critical stage of its implementation, resulted in change, quality, risk and contract management issues not being resolved on a timely or effective basis. The Program Director had intimate knowledge of CJEP and its stakeholders and the necessary experience to effectively manage a large and complex IT project. This situation was addressed in October 2003.
- The department has not fully acted on the recommendation made in our 2003 report to Parliament on CJEP to strengthen its governance arrangements through greater independent oversight by having an independent body such as the department's audit committee providing independent scrutiny. While not involving an independent body such as its audit committee, the department has periodically engaged consultants to review and advise the steering committee on the overall progress and specific aspects of CJEP.
- Key documents and reports that were endorsed by the steering committee, subject to certain changes being made, were not re-presented at a subsequent meeting in their final form for final adoption or approval. In these circumstances, it was difficult to ascertain which version was the final document or report.
- The CJEP Quality Management Plan (September 1999) and the CJEP Risk Management Plan *(*December 2000) included relevant and comprehensive principles and processes to facilitate adequate project management of CJEP and we saw evidence of periodic reporting against these plans and a change management plan to the CJEP Steering Committee. However, there was limited evidence that these plans were effectively implemented during the period February 2002 to October 2003, a critical stage of CJEP's implementation.

While high level partner agency commitment to the CJEP program was always present in a formal sense through membership of the CJEP Steering Committee and allocation of internal resources by agencies to support the program, this was not always matched by actions and 'on the ground' commitment and ownership.

The level of commitment by some partner agencies was questioned by both the chairperson and the CJEP Program Director at various stages at committee meetings. Ultimately, the timely and successful completion of CJEP was partly dependent on the partner agencies and the CJEP Steering Committee did not have the authority to compel commitment and ownership by agencies, its powers were essentially persuasive.

Early problems with the quality, stability and reliability of CJEP applications rolled out into agencies for testing, whether caused by poor supporting IT infrastructure or contractor performance issues, damaged the confidence of agency staff in the CJEP program.

The ongoing governance arrangements for CJEP are set out in the June 2006 CJEP Memorandum of Understanding (MOU) and are appropriate. The CJEP partner agencies, except Victoria Legal Aid (VLA), have signed the MOU to signify their agreement to comply with its provisions. VLA is expected to sign the MOU when it becomes an active user of CJEP systems.

5.4 CJEP monitoring and reporting

Monitoring and reporting the progress, deliverables and outcomes of a large and complex program such as CJEP is critical to its effective oversight and management and impacts on whether an overall assessment of the success of the program's implementation can be undertaken by project stakeholders including ministers.

The CJEP Project Definition developed in August 1999 provided the basis for the program's cost and financial management framework and specified the following monitoring and reporting processes:

- The Program Director and key contractor(s) responsible for major deliverables were required to provide status reports to the steering committee including:
  - overall program status including budget performance (month and year to date actual against budget), schedule and deliverables
  - completion rate by project
  - release program for entire program
  - key risk summary
  - implementation and agency issues.
- The Program Director was required to provide regular briefing papers to the project champion at least monthly and the ministers as required.
- The department was required to provide quarterly reporting to the Department of Treasury and Finance (DTF) during the term of the project.

We found that the majority of these monitoring and reporting processes were established. However, our review of various documents and reports including the CJEP Steering Committee minutes, funding submissions and briefing papers to the project champion and relevant ministers identified a number of deficiencies.

Adequacy of reporting to CJEP Steering Committee

Reporting by the CJEP Program Director to the steering committee, particularly in the earlier phase of the program's implementation, was consistent with the CJEP's Project Definition requirements. However, it lacked sufficient detail to facilitate the level of oversight and management required for such a large and complex project.

Reporting to the steering committee was strengthened in 2003 when consultants were engaged by the department to review CJEP and were also required to provide monthly status reports to the steering committee commencing in October 2003. The content of these status reports was comprehensive and informative. They ceased in November 2005 on the basis that development work on CJEP's core projects, with the exception of E*Brief, had been completed by that time.

Failure to monitor whole of project costs

There is no monitoring and reporting of the program's whole of project and whole of life project costs incurred by the department and other agencies.

The department does not monitor and report the program costs incurred by partner agencies. This is despite the recommendation made in our May 2003 report that the department determines, monitors and reports on total program expenditure (including the costs incurred by partner agencies) so that the aggregate program costs could be included in the department's annual report to Parliament.

Based on information provided by some CJEP partner agencies, they have incurred costs in excess of $10 million in CJEP ongoing maintenance and support costs over and above what has been spent by the department. The Magistrates' Court, OPP and VLA did not provide us with information on costs they have incurred in implementing CJEP systems.

Failure to report regularly to DTF

Despite CJEP's August 1999 Project Definition indicating a requirement for the department to provide a quarterly progress report to DTF during the term of the project, this has not occurred.

5.5 Overall conclusion

The department has demonstrably placed significant emphasis on the governance and management arrangements for CJEP since its inception and these arrangements largely met audit expectations, specifically:

- the CJEP Steering Committee had adequate stakeholder representation, and was provided with regular reporting on the program's progress
- the department took appropriate action to strengthen CJEP's governance and management structures in response to recommendations made in our May 2003 report to Parliament on the progress of CJEP.

Appropriate governance and management structures and arrangements do not, on their own, guarantee the success of any major project. There also needs to be real commitment to and ownership of the project by the stakeholders and agencies tasked with implementing it.

While high level partner agency commitment to the CJEP program was always present in a formal sense—through membership of the CJEP Steering Committee and allocation of internal resources by agencies to support the program—this was not always matched by actions and 'on the ground' commitment and ownership.

We identified deficiencies in the application and enactment of the CJEP governance and management arrangements and in CJEP's monitoring and reporting framework that adversely affected the oversight and management of CJEP's implementation and assessment of the expected program and project deliverables and outcomes.

6 Ongoing management and support of CJEP systems

At a glance

Background

The Department of Justice (the department) needs to ensure the provision of effective ongoing support and management of CJEP systems to realise their benefits.

Key findings

The department developed and implemented an effective plan to transition the future development and support of CJEP from the primary IT contractor to the department's in-house support group. However, the decision to provide the ongoing support service for CJEP systems internally was not based on a comprehensive and fully costed business case.

The department lacks a CJEP specific risk management strategy, risk register and risk plans to identify, manage and monitor the ongoing maintenance and support risks relating to the CJEP systems.

The department developed a memorandum of understanding (MOU) in June 2006 to define the governance policies and arrangements for the oversight, management and coordination of the CJEP as an ongoing program. This MOU has been operational since June 2006 and has been signed off by all partner agencies except Victoria Legal Aid (VLA), which is not an active user of CJEP systems yet.

Although the department has implemented governance and management structures and processes to support the provision of ongoing maintenance, support and enhancement of the CJEP systems, these need to be further strengthened. In addition, the decision to continue to provide the service internally needs to be reviewed and adequately justified.

At a glance – *continued*

Key recommendations – *continued*

The department needs to:

- obtain sign off to the MOU by VLA to formalise the governance arrangements in place relating to CJEP
- develop a comprehensive and fully costed business case including an option analysis to justify funding levels and whether the CJEP support service should be retained internally or be outsourced
- develop and maintain a risk management strategy and risk plans to identify, manage and monitor any ongoing risks relating to CJEP systems. **(Recommendation 6.1)**

6.1 Background

Provision of adequate ongoing post-implementation support is critical for major IT projects such as CJEP.

CJEP's original October 1998 budget included $1.4 million per year for the maintenance and ongoing support and operation of the CJEP systems for the period up to 30 June 2003. This support function was initially delivered by the primary IT contractor. The contractor ceased performing the support function in September 2005. Since then the department has provided support services using internal resources.

We expected to find an appropriate governance and control structure in place to oversight the ongoing management, support and operation of CJEP systems, including:

- clear roles, responsibilities and accountabilities for systems and data 'ownership' and security
- an appropriate organisational and/or contractual structure for the ongoing maintenance and support of CJEP systems
- ongoing program cost monitoring, ensuring that costs are consistent with plans and the business case
- clear CJEP systems maintenance and support plans and programs, and these should be adequately resourced and funded
- an effectively implemented comprehensive training/change management plan to achieve a 'smooth' transition from outsourced IT support to in-house IT support.

6.2 Transition process

The department undertook an effective process to ensure a smooth transition from the primary IT contractor responsible for the development of the CJEP systems to the in-house Integrated Justice Systems (IJS) unit. A transition plan was agreed with the IT contractor and a transition team was announced in mid-May 2005. The transition process took place over a three month period, concluding on 30 September 2005 just prior to the expiry of the IT contract in November 2005.

The transition process involved a strategy for the IT contractor to complete the main contract work, outstanding change requests and to prepare the IJS unit to continue to develop and support the CJEP program, including the transfer of all contracted materials and knowledge.

6.3 CJEP future governance structure

Proposed governance structure

A proposed future governance structure for the CJEP program is detailed in a memorandum of understanding (MOU) between the department and partner agencies, dated June 2006. The purpose of the MOU is to define the governance policies and arrangements for the oversight, management and coordination of the CJEP program as an ongoing program. It addresses various aspects including:

- governance
- notification and change control procedures
- information exchange protocols
- privacy policy
- information security policy
- business continuity plans
- reporting arrangements
- MOU operative period and review process
- service level agreements and performance targets.

The MOU was endorsed by the CJEP steering committee in June 2006 and has been signed off by all the partner agencies, except VLA which is not yet an active user of CJEP systems. VLA is concerned that the MOU prohibits the emailing of information through the internet to defence lawyers and the OPP. VLA has argued that this is a normal part of their business and would be very restrictive. VLA and the department are continuing discussions to resolve this issue.

The new governance structure outlined in the MOU includes the following changes to the existing CJEP governance structure:

- a change of name for the CJEP Steering Committee to the CJEP Governance Board with its composition expected to remain unchanged although its focus will be more on the operational aspects of CJEP rather than the delivery of CJEP's IT systems
- a changed role for the CJEP Program Director to involve reporting to the governance board while ensuring broader reform and maintenance of the CJEP program's momentum
- continuation of a change control board which has been operational since the creation of the IJS unit
- creation of four new committees namely the:
  - Security and Privacy Committee
  - Situation Response Committee
  - Program Monitoring and Benefits Capture Committee
  - Architecture and Infrastructure Committee.

The department advised that the committees supporting the CJEP Governance Board have been consolidated into the Information Security and Privacy Committee, the Operational Management Committee and the Architecture and Planning Committee.

While the new governance structure has been established and communicated to partner agencies it is not fully operational because the CJEP Governance Board has not met and the supporting committees are yet to meet on a regular basis. The department advised that meetings of the Governance Board and committees are to be scheduled for mid-2008.

CJEP risk management strategy and plans

Developing and maintaining a risk management strategy and risk plans where relevant risks are identified and rated and treatment plans are devised to mitigate these risks is central to effective risk management practice.

Currently there is no documented risk management strategy, risk register or risk plans maintained by the IJS unit or the department's Technology Services division to identify, manage and monitor any risks relating to the ongoing operation of CJEP systems. Furthermore there is no plan as part of CJEP's new governance structure to develop and maintain a risk management strategy and risk plans.

6.4 Establishment, funding and monitoring of IJS unit

Funding and establishment of IJS unit was not based on a detailed business case

An amount of $1.4 million per annum of projected recurrent expenditure was approved as part of the original CJEP budget in October 1998 to maintain and operate the CJEP systems up until June 2003.

In September 2003 this budget was reviewed and revised to $5.6 million, by consultants engaged by the department. The department was not able to provide audit with the information or data provided to the consultant used as the basis for determining the revised budget. This funding supplementation was endorsed by the CJEP Steering Committee in late 2003 and funding was secured from the department's existing budget**.** The Secretary of the Department wrote to all participating agencies in February 2004 stating that funding had been secured from existing departmental funds.

The funds required for the annual support and management of CJEP systems was revised upwards by the CJEP Program Director in 2005–06 to $6.4 million per annum. Some of the adjustment was to provide for costs relating to the capital assets charge and related depreciation costs which were omitted from the amount determined by the consultant. This request for additional funding was endorsed by the CJEP Steering Committee in March 2005.

The CJEP Steering Committee also endorsed the decision to fund the establishment of the IJS unit within the department rather than outsource the provision of support services for CJEP systems. This decision was based on a presentation by the CJEP Program Director to the committee that outlined the proposed structure, resources and budget for the IJS unit. The presentation included a comparison of the expected costs associated with both in-house and the existing outsourced support services and indicated that based on previous experience with the primary IT contractor used for CJEP's implementation it would be more cost effective to provide the support services internally.

While the CJEP Steering Committee was provided with a presentation and supporting paper comparing the expected costs of an in-house support service with the costs of the existing outsourced support service, this advice would have been more comprehensive if the costs of outsourced support services from providers other than the incumbent primary IT contractor had been obtained and included in the analysis.

It is anticipated that ongoing funding requirements for the IJS unit will be reviewed when CJEP is fully implemented and the new governance structure is fully operational. However, the department has advised there are no plans to prepare a cost benefit analysis to evaluate if the functions currently performed by the IJS unit should remain in-house or be outsourced.

Monitoring of IJS unit costs

The IJS unit allocates specific resources to its various activities based on expected workload requirements for known tasks and past experience of patterns of demand for support services for CJEP systems. For major development and maintenance tasks this is underpinned by specific output targets, time and cost budgets.

The IJS unit has an adequate costing system in place to ensure total costs related to its key responsibilities of providing ongoing maintenance, support and enhancements to the CJEP systems are captured, recorded, accounted for and monitored.

The IJS unit's overall budget is monitored and reported as part of the department's Technology Services' group and there was also reporting of the IJS unit's performance and costs to the CJEP Steering Committee.

While IJS unit costs are captured and monitored at the overall level and for significant projects and development tasks, the department could not provide a detailed breakdown of the actual costs of its main activities incurred since January 2006:

- ongoing maintenance and support for work performed on implemented CJEP modules
- development of enhancements to the IJS suite of applications.

The department provided an estimated breakdown of total IJS unit costs by key responsibility area based on its knowledge of the proportion of IJS unit staff time typically spent in each area. In audit's view it would be useful for the CJEP Governance Board to be provided with regular reporting on both total costs incurred by the IJS unit and on the breakdown of those total costs into actual costs incurred by main activity area. This would inform the Governance Board about changes in the costs incurred over time in supporting, developing and maintaining CJEP systems and facilitate questioning and decision making by the board on the focus and balancing of the IJS unit's work effort and resourcing.

Recommendation

6.1 The department needs to:

- obtain sign off to the MOU by VLA to formalise the governance arrangements in place relating to CJEP
- develop a comprehensive and fully costed business case including an option analysis to justify funding levels and whether the CJEP support service should be retained internally or be outsourced
- develop and maintain a risk management strategy and risk plans to identify, manage and monitor any ongoing risks relating to CJEP systems.

7 Information security over CJEP

At a glance

Background

CJEP involved the creation of new information systems, the modification of pre-existing information systems and their implementation and integration across multiple partner organisations within Victoria's justice system. These systems store information, including personal information on individual citizens, which is highly sensitive and must be properly secured.

Key findings

A comprehensive overarching information security policy for CJEP systems and information was established in June 2006. Some of the actions required under that policy have not been implemented. While this is not a desirable situation and needs to be addressed, information security policies and controls over CJEP systems are in place at the individual agency level.

The CJEP MOU which was finalised in June 2006 and includes the CJEP Information Security Policy and privacy policy has been signed by all partner agencies actively using CJEP systems.

The Department of Justice (the department) has recognised the need for a more comprehensive approach to information security over the past two years and has taken positive steps to address weaknesses in its previous approach.

Notwithstanding this, the department needs to maintain a strong focus on ensuring that its information security management system is fully implemented and monitored for effectiveness and compliance. The department is in the process of:

- supporting the communication of the new Information Security Management System framework (ISMS) and policies to all staff, contractors and relevant partners with a coordinated training program
- completing a 'gap analysis' to identify the extent to which current practices and controls meet the requirements of the new framework and policies
- fully implementing data classification that is critical to the effectiveness of any ISMS.

At a glance – *continued*

Key recommendations

The CJEP Information Security and Privacy Committee should commence regular annual reporting to the CJEP Governance Board on any breaches of policy or any other issues that may impact on CJEP systems. **(Recommendation 7.1)**

The department should

- ensure that the information privacy statements of CJEP partner organisations comply with the requirements of the CJEP Information Security Policy **(Recommendation 7.2)**
- establish a business continuity plan for the shared domain elements of CJEP systems **(Recommendation 7.3)**
- ensure that its data classification scheme is fully implemented and supported with appropriate guidance material as soon as possible **(Recommendation 7.4)**
- establish performance measures for the management of information security and ensure that subsequent performance is monitored and reported to senior management **(Recommendation 7.5)**
- finalise the development of an overall IT security plan that covers the building of awareness, establishes clear standards based on its Information Security Policy and ICT Security Policy, and defines monitoring and enforcement processes **(Recommendation 7.6)**
- establish a single configuration management database as soon as possible. **(Recommendation 7.7)**

7.1 Background

To perform their functions effectively public sector agencies need to collect, create, use and hold a wide range of information, including personal information on individual citizens. The community expects these agencies to secure and to use that information appropriately. There are also legal requirements, such as privacy legislation, which set standards for the collection and handling of personal information by the public sector.

CJEP involves both the creation of new information systems, the modification of pre-existing information systems and their implementation and integration across multiple partner organisations within Victoria's justice system. These systems store information, on individual citizens, which is highly sensitive and which must be properly secured. As part of this audit we examined whether CJEP systems and data are secure, and whether information security and privacy arrangements were consistent with relevant legislative requirements.

The CJEP systems are referred to collectively as the Integrated Justice Systems suite of applications or the Integrated Justice Systems (IJS). The adequacy of security over IJS systems and data is ultimately in the hands of the individual justice sector agencies and their staff, contractors and partners who use the systems. These agencies need to establish, maintain and adhere to effective information security management systems.

There is also a need for an overarching information security policy and system governing the CJEP or IJS suite of applications given the multi-agency nature of the CJEP and the fact that IJS systems involve the exchange and sharing of information within and between agencies. There should be clearly documented standards for the protection and security of IJS systems and data so that affected agencies have a common understanding and reference point on the minimum standards required. The policies and systems of individual agencies should be consistent with the overarching requirements.

As part of this audit we examined both the overarching framework for CJEP information and system security and the policies and practices of the department. This part of the report outlines the results of that work and includes observations on specific aspects of the adequacy of information security policies, systems, controls and practices impacting on the CJEP information and systems.

7.2 Overarching framework for CJEP information and system security

CJEP has established several key computer systems including the E*Justice system, SCT Courts and the Justice Knowledge Exchange (JKE). These systems, which account for a major proportion of the IJS, operate in conjunction with a large number of legacy systems and reside in a complex set of networks in Victoria Police and the Department of Justice. IJS also includes secure links between Department of Justice, Victoria Police, Office of Public Prosecutions, Corrections Victoria and private prison providers to enable the sharing of information.

As previously indicated, the adequacy of security over IJS systems and data is ultimately dependant on the CJEP partner organisations in the justice sector. These agencies need to establish, maintain and adhere to appropriate information security management systems. In addition, all CJEP partner organisations are bound by the directions of the Commissioner for Law Enforcement Data Security[1] in connection with any access they have to Victoria Police law enforcement data repositories.

We also identified a need for clearly documented standards for the protection and security of IJS systems and data so that affected agencies have a common understanding of minimum standards.

In June 2006 the CJEP Memorandum of Understanding (MOU) was established to define the governance policies and arrangements for the oversight, management and coordination of CJEP as an ongoing program. The MOU includes both an information security policy and a privacy policy for CJEP. These policies were agreed 'in principle' by the CJEP Steering Committee, which includes representatives from all CJEP partner agencies. The MOU also included a commitment to establish a CJEP Security and Privacy Committee.

CJEP partner agencies were expected to sign the MOU and agree to comply with its provisions, including the privacy and information security policies. To date, the MOU has been signed by all partner agencies except Victoria Legal Aid (VLA). The department advised that VLA has not signed the MOU because it is not a current user of CJEP systems and due to concerns about the content of, or their ability to comply with certain aspects of, the CJEP Information Security Policy.

[1] The Commissioner for Law Enforcement Data Security commenced in July 2006 under the *Commissioner for Law Enforcement Data Security Act* 2005. The principle purpose of the Act is to promote the use by the police force of Victoria of appropriate and secure management practices for law enforcement data. One of the Commissioner's functions under the Act is to establish standards for the security and integrity of law enforcement data systems.

7.2.1 CJEP Information Security Policy

The CJEP MOU includes the CJEP Information Security Policy and states that the policy sets out the guiding principles and strategies for the IJS suite of applications to enable appropriate levels of system and information availability, integrity and confidentiality to be achieved. The policy is designed to ensure that:

- appropriate, cost effective safeguards and procedures are adopted to protect IJS information system resources
- all responsible personnel, contractors, service providers and/or vendors are aware of their accountability and responsibility for the effective implementation and operation of these safeguards
- auditability of system use, safeguards and procedures applying to IJS information system resources is facilitated.

The CJEP MOU states that CJEP partner organisations are obliged to comply with the CJEP Information Security Policy and that compliance with the policy is mandatory for all personnel who access, or have responsibility for the development, implementation and/or support of IJS application suite information system resources.

The CJEP Information Security Policy is intended to form an extension of the information security policies in place at Victoria Police and the department and its purpose is to complement, but not replace, these policies in their respective IT domains. The policy states that in the event of any gap or inconsistency between these policies, the CJEP policy will be the authoritative policy statement for information security within the CJEP shared domain.

We reviewed the CJEP Information Security Policy against our expectations of such policies, which are drawn from a range of sources including accepted national and international standards[2] and guidelines, and concluded that it is adequate. Key elements of the policy include:

- policy framework
- information security—organisation and responsibilities
- education and awareness training
- general user access controls
- network security
- system integrity
- data security and privacy
- compliance
- CJEP security governance.

In addition, the CJEP Information Security Policy adequately addresses the requirements of the relevant security and privacy legislation.

---

[2] Australian standard AS/NZS 7799.2:2003 *Information security management—Specification for information security management systems.* ISO 27001:2005 *Information technology—security techniques—Information security management systems—Requirements. Australian Government Information Technology Security Manual, ASCI 33.*

A policy may be comprehensive but it is only a document and will have no effect if it is not effectively communicated to and implemented by the responsible organisations and people. The CJEP Information Security Policy states that:

- all designated users of CJEP applications will be required to complete training in the proper use of such applications and the security responsibilities and controls to which they are subject
- supervisors must receive training and guidance on their responsibility to ensure that staff follow proper information security procedures
- all employees must be made aware of:
  - user access controls and responsibilities
  - procedures for reporting security incidents, weaknesses and software/hardware malfunctions
  - disciplinary procedures when sponsoring organisation policies and procedures are deliberately disregarded or violated.

Relevant staff of the department, partner agencies and third parties such as private prison operators are provided with training on the requirements of the CJEP Information Security Policy.

Information exchange and network security

An important part of CJEP's purpose is the exchange of information between justice sector agencies. The CJEP MOU documents the protocols for the sharing and exchange of information and states that:

- CJEP will facilitate the routine exchange of structured information sets according to agreed protocols between partner organisations
- the information exchange protocols are formalised in structured message and software routines in the Justice Knowledge Exchange (JKE) application, which regulates the exchange of information between E*Justice, CLMS (Courts) and each partner organisation's legacy systems
- the responsibility for the ongoing monitoring and review of the integrity of these messages rests with the IJS unit within the department
- the CJEP Governance Board will formally review the information management and exchange protocols every twelve months.

These protocols are reinforced and expanded on in the CJEP Information Security Policy. The policy also specifies network security requirements. These requirements cover external third party connections to IJS applications in the CJEP shared domain. The policy requires that before such access is approved, the third party connecting network must be certified as meeting certain defined minimum conditions for a secure network.

Data security and privacy

The proper classification of data is absolutely fundamental to maintaining data security. Australian information security standards indicate that an adequate data classification scheme should be established to facilitate the development of an Information Security Management System (ISMS). The role of data classification within an ISMS security management framework is to 'tag' information resources with a category that indicates the level of risk associated with the compromise of that resource. Security controls that mitigate that risk should be implemented in accordance with the classification level. Compromise of the data classification scheme may result in inappropriate disclosure of data, consequential loss and damage.

The CJEP Information Security Policy requires that CJEP data and/or information must be classified according to its degree of sensitivity, confidentiality and criticality. The policy imposes responsibility on the relevant system sponsor for establishing the classification of end user data and/or information created in CJEP related systems. The department approved a data classification scheme in March 2007 and has communicated the scheme requirements to businesss units and staff. The department is in the process of developing guidelines for departmental staff about the appropriate controls to be applied to the various categories of data.

The policy further states that CJEP shared domain data will be classified according to criteria established by the CJEP Information Security and Privacy Committee. This committee is responsible for the establishment and monitoring of Security and Privacy policies and standards and for their effective communication to all CJEP partner organisations. The committee has not issued data classification criteria.

The department advised that the classification criteria to be applied to CJEP data is detailed in the department's approved data classification scheme. The CJEP Information Security and Privacy Committee should formalise and communicate this decision to ensure clarity about the data classification scheme for CJEP shared domain data and the consistency with which partner agencies treat and secure CJEP information.

The CJEP Information Security Policy requires that all CJEP partner organisations' information privacy statements include a description of how data stored in or utilised by CJEP Shared Domain systems will be managed in accordance with the principles (IPP's) contained in the *Information Privacy Act* 2000.

The policy further requires CJEP partner organisations to report any known instances of non-compliance with their Privacy Statement to the CJEP Governance Board and to proactively assist with the timely resolution of any matters raised for investigation. The policy also commits the CJEP Information Security and Privacy Committee to reporting annually to the CJEP Governance Board on any breaches of policy or any other issues that may affect CJEP systems. This has not occurred as yet. The department advised that a report will be submitted to the CJEP Governance Board in July 2008.

Recommendations

7.1 The CJEP Information Security and Privacy Committee should commence regular annual reporting to the CJEP Governance Board on any breaches of policy or any other issues that may affect CJEP systems.

7.2 The department should ensure that the information privacy statements of CJEP partner organisations comply with the requirements of the CJEP Information Security Policy.

Business continuity planning

The CJEP Information Security Policy requires the department's IJS unit to maintain a business continuity plan (BCP) for all shared domain elements of CJEP systems. This is particularly important given the significance and sensitivity of these systems. However, a BCP for the shared domain elements of CJEP systems has not yet been established.

The stated purpose of the BCP for shared domain CJEP systems is to document procedures that ensure:

- interruptions to service are minimised
- recovery of failed systems (including the data/information managed by the systems) can be effectively and efficiently achieved
- personnel and providers in CJEP partner organisations can work effectively together around a common plan.

The CJEP BCP is complementary to BCPs required by CJEP partner organisations under their respective IT domains. It does not replace these BCPs and we were advised by the department that both it and the County Court have BCPs.

The CJEP Information Security Policy also requires CJEP system sponsors to document and maintain effective Information System Contingency Plans for the minimisation of service interruptions and the recovery of failed systems for all CJEP related information systems. These plans must be adequately tested and reviewed and, where necessary, revised on a regular basis (recommended annually).

Recommendation

7.3 The department should establish a business continuity plan for the shared domain elements of CJEP systems.

Performance reporting against CJEP Information Security Policy

The CJEP Information Security Policy states that the CJEP Governance Board, supported by the CJEP Information Security and Privacy Committee has overall responsibility for overseeing CJEP security policy and ensuring comprehensive procedures are maintained for monitoring compliance with the policy.

The CJEP MOU requires the presentation of bi-monthly reports to the board and partner organisations setting out operational performance of the CJEP systems, non-compliance issues and notifications.

The CJEP Information Security Policy also mandates the undertaking of an annual security review of compliance with the policy and its supporting procedures. The department advised that that the results of the annual security review would be reported to the CJEP Governance Board by July 2008.

7.3 Information security at individual agencies

While there is an overarching information security policy for CJEP information and systems we have previously indicated that the adequacy of security over these systems and data is ultimately in the hands of the individual justice sector agencies and their staff, contractors and partners who use the systems. These agencies need to establish, maintain and adhere to effective information security management systems.

We examine the adequacy of information security policies, controls and practices in public sector agencies, including justice sector agencies, routinely as part of our financial audit processes and report our findings and any recommended improvements to the management of these agencies and to Parliament where warranted.

Our December 2007 report to Parliament on the results of financial statement audits for agencies with 30 June 2007 balance dates included commentary on the adequacy of information system (IS) controls in justice sector agencies and indicated that our audits found that agencies had established:

- appropriate IS controls over most aspects of IS operations
- adequate procedures to document changes to networks and applications
- adequate procedures for IS continuity planning.

In this audit we focussed on the adequacy of the department's information security systems policies and controls.

7.3.1 Adequacy of the Department of Justice information security systems

The CJEP systems function in a very complex environment that features multiple platforms, multiple vendors, and complex automated processes, which in turn manipulate sensitive data. Accordingly, the department requires sophisticated security controls to be established to ensure that its information security policy requirements are complied with.

We found that the department has recognised the need for a more comprehensive approach to information security over the past two years and has taken positive steps to address weaknesses in its previous approach to this important aspect of its operations. There is clear evidence of a commitment by the department to undertake the work necessary to ensure that its information security policies and practices meet better practice and recognised standards.

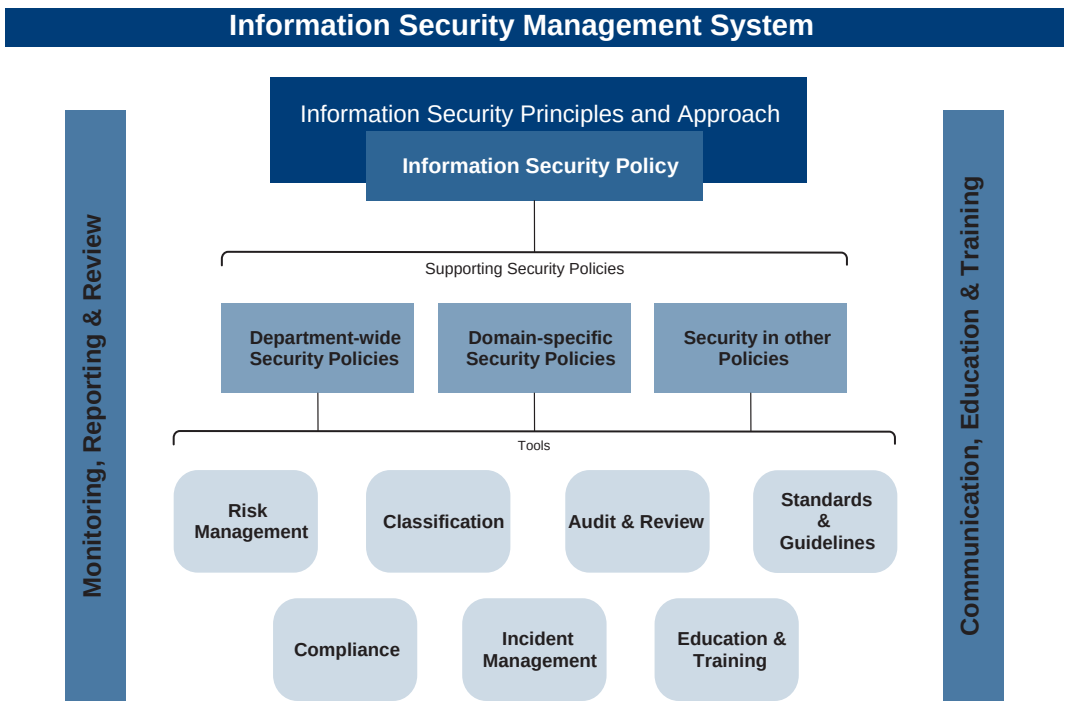
Notwithstanding this, the department needs to maintain a strong focus on ensuring that its information security management system is fully implemented and monitored for effectiveness and compliance.

The department's previous IT security policy was established in 2001 but was not widely disseminated within the department, creating a risk that staff and service providers who were unaware of the policy may not act in accordance with it. The failure to communicate clear policy directions concerning information security increases the risk of a security failure and subsequent compromise of the integrity, confidentiality and availability of programs and data.

The department's Knowledge Management Committee (KMC) endorsed the Information Security Management System (ISMS) framework for the department in July 2006. The ISMS is not a single document but a framework that includes policy documents and specific tools and management practices. The development of an ISMS is a requirement of the *Whole of Victorian Government Standard on Information Security Management*[3]. The department's ISMS is shown in Figure 7A.

[3] This standard was issued by the Victorian government Chief Information Officer in 2005.

Figure 7A
Department of Justice Information Security Management System



Source: Department of Justice.

The department has been progressively implementing the ISMS since it was endorsed in July 2006. The department approved an Information Security Policy in July 2006 and an ICT Security Policy in August 2007.

We found the department's ISMS framework and the supporting policies to be comprehensive and consistent with the requirements of the CJEP Information Security Policy.

The department is in the process of:

- supporting the communication of the new ISMS framework and policies to all staff, contractors and relevant partners with a coordinated training and awareness program
- completing a 'gap analysis' to identify the extent to which current practices and controls meet the requirements of the new framework and policies
- fully implementing data classification which is critical to the effectiveness of any ISMS.

The department's ISMS includes a data classification scheme, as part of its Information Security Policy, covering data in IT systems, physical data, documents and removable data storage devices and media. The department's data classification scheme was approved in March 2007 and is consistent with that used by the Victoria Police.

The department has communicated the data classification scheme requirements to businesss units and staff and is in the process of developing guidelines for departmental staff about the appropriate controls to be applied to the various categories of data. This work needs to be expedited to ensure the scheme is fully implemented and operationalised in the department to provide assurance about the maintenance of adequate controls over all departmental IT systems and data, including CJEP related systems and data.

We also found that the department does not currently meet certain requirements of external standards quoted in its policy statements, including: ACSI 33, physical standards for technology and the Protective Security Manual.

In terms of clarity about ownership and therefore accountability for security over the data held in CJEP systems, the department advised that:

- data in shared systems such as E*Justice is owned by the Secretary of the department as sponsor of CJEP
- data contained in the CLMS system is owned by the Chief Judge as head of that jurisdiction
- arrangements for ownership of data in legacy systems that CJEP systems connect with, such as the Victoria Police Law Enforcement Assistance Program (LEAP) database, have not been disturbed.

Recommendation

7.4 That the department ensure that its data classification scheme is fully implemented and supported with appropriate guidance material as soon as possible.

Monitoring of compliance with information security policies

Prior to 2007 there was limited evidence that the department's senior management were actively monitoring and periodically reassessing information security compliance and performance on a regular basis to ensure that policies continued to be appropriate and that controls were accomplishing their intended purpose.

This weakness was substantially addressed in March 2007, when the department established the Information Security Management Committee (ISMC). The responsibilities of this committee include advising and reporting to the Risk and Compliance Committee on compliance and risk issues with regard to information and ICT security.

However, although senior management receives regular reports of security failures the department has not established performance indicators for IT security issues. The development and monitoring of such performance indicators is important to assist the ISMC fulfil its functions.

Recommendation

7.5 The department should establish performance measures for the management of information security and ensure that subsequent performance is monitored and reported to senior management. Suitable performance measures include:

- number of security related service calls, change requests and fixes
- amount of downtime caused by security incidents
- turnaround time for security administration requests
- number of systems subject to an intrusion detection process
- number of systems with active monitoring capabilities
- time to investigate security incidents
- time lag between detection, reporting and acting upon security incidents
- number of information security awareness training days.

Lack of an IT security plan

Additionally the department's ISMS is weakened by the absence of an IT security plan for CJEP. A consultant engaged by the department to examine its sensitive information and data management processes recommended in December 2005 that the department complete and approve an IT Security plan for E* Justice. This recommendation has not been implemented. The department advised that an IT security plan is being developed by its ISMC.

Recommendation

7.6 The department should finalise the development of an overall IT security plan that covers the building of awareness, establishes clear standards based on its Information Security Policy and ICT Security Policy, and defines monitoring and enforcement processes.

Lack of a configuration management database

The Australian standard *AS/NZS 7799.2:2003 Information security management—Specification for information security management systems* recommends that an inventory of all important assets associated with each information system be drawn up and maintained.

We found that while the department's IT services contractor and departmental staff have a number of databases and spreadsheets identifying the department's information technology assets and there is a separate tracking mechanism that enables the monitoring of charges for the provision of services related to information technology assets, the department does not maintain a single formal configuration management database. The lack of a configuration database, corresponding with the schedule of ICT equipment maintained by the outsourcing contractor, increases the risk of information technology assets, containing sensitive programs and data, not being correctly configured to manage security threats.

Recommendation

7.7 That the department establish a single configuration management database as soon as possible.

Security requirements in outsourcing contracts not fully implemented

The department has outsourced the management of the department's ICT infrastructure, data centre, servers, network and end-user environments to a service provider.

Section A.4.3.1, Security requirements in outsourcing contracts of Australian standard AS/NZS 7799.2:2003 *Information security management - Specification for information security management systems* recommends that:

> *'The security requirements of an organisation outsourcing the management and control of all or some of its information systems, networks and/or desktop environments shall be addressed in a contract agreed between the parties.'*

The department has provided a clear and current statement of its ICT security requirements for CJEP programs and data to the contractor and has also established controls that require changes to be implemented by the contractor only after agreement by the department's security personnel.

However, the department's contract with the IT service provider needs to be updated to:

- reflect the requirements of the department's security policies, the *Privacy Act* 2000 and the risks introduced along with the new technology implemented to support CJEP programs and data
- include a current list of IT equipment to be maintained and other services to be provided. The lack of a current list of equipment will increase the risk that the department may be unable to approve contractor invoices, manage security patching and vendor updates or maintain its risk register for CJEP IT assets.

Limited segregation of duties impacting on CJEP software

We found that arrangements for the segregation of duties could be improved to provide better control over changes to key CJEP software including the Justice Knowledge Exchange (JKE) program.

The department has arrangements in place to segregate the duties and responsibilities of developers to reduce the risk of unauthorised changes to CJEP data or programs. The department has also established enhanced security checks on IKS staff and has non-disclosure agreements in place. In addition, the department has work flow and approval control procedures established to control changes introduced by its webMethods Development Team.

Notwithstanding these controls, we found a potential weakness in controls because two IKS support staff and the webMethods contract developer have access to both the Department of Justice's and Victoria Police's development and production networks and to both agencies' webMethods development environments. They can also access the webMethods production Web servers and JKE software and are able to initiate work, complete work and finally deploy the completed changes into production. Allowing developers access to production and development environments and to the ability to deploy completed works into the production environment increases the risk of unauthorised changes to production software.

Recommendation

7.8 That the department review how webMethods programming duties are organised to reduce the risk of unauthorised changes to production software.

Identity management and access control system

The department has not established a comprehensive identity management and access control system. The department has recognised this and has obtained funding to allow it to establish a suitable system, which may be based on its implementation of the Rosetta solution. Rosetta is an integrated electronic directory infrastructure for the whole of Victorian Government.

Miscellaneous issues

In addition to the issues reported above, we also communicated a range of other matters to the department during the course of our audit regarding potential improvements in its IT security practices including:

- risk assessment and management practices
- the need for clarity in the contractual arrangements with its primary IT service provider
- the need for more regular external vulnerability assessments and scans of its IT systems

- password security in application-to-application programming and other password and access related issues.

7.4 Inappropriate access to or use of data on CJEP and related systems

The department has appropriate controls in place to both inform relevant staff about their obligations and to identify and investigate potential instances of inappropriate access to or use of data on CJEP and related systems.

Based on the information examined in our audit there has only been one significant inappropriate data access event involving the implementation of CJEP. This occurred at Corrections Victoria in late 2004.

The E*Justice application was initially made available to Corrections Victoria staff in November 2004. E*Justice is one of the CJEP IT systems and is used by Corrections Victoria staff to manage prisoners and offenders. The E*Justice application regularly draws on information from the Victoria Police LEAP database, and in turn, updates LEAP with information entered into it by Corrections staff.

Audits of use of E*Justice revealed that 22 community corrections staff appeared to have inappropriately accessed information in the LEAP database during the period November and December 2004. The department took appropriate action to investigate this matter and the investigation indicated that 15 of the 22 staff had inappropriately accessed LEAP data. In all 15 cases the staff members had accessed their own records or records of members of their families. The remaining seven staff had legitimately accessed records in LEAP to confirm the identity of offenders who formed part of their case loads. Formal warning letters were sent to the 15 staff who had inappropriately accessed LEAP data.

Appendix A.
Department of Justice response on audit conclusions

Department of Justice response

RESPONSE provided by Acting Secretary, Department of Justice

The report contains a number of conclusions with which the Department fundamentally disagrees. While the Department acknowledges that these conclusions are audit opinion, it does not believe that they are supported by the facts. These conclusions are set out below:

1998 Business Case

The report concludes that the business case for CJEP which was developed in 1998 was inadequate and that this contributed to delays in completing CJEP.

The Department acknowledges that the original business case for CJEP, which was completed in 1998, is not consistent with the standard for business cases which would apply now. It notes, however, that the business case for the project was revised at key stages as changes in the criminal justice environment emerged. The Department believes that it is important to regularly review business case assumptions for all complex ICT enabled projects, particularly where implementation extends over a number of years.

FURTHER comment by the Auditor-General

The department's response does not present any facts which would call into question, or invalidate the audit conclusion.

The criteria set out in section 3.1 of the report against which the audit assessed the 1998 business case are common sense criteria and are not overly onerous or sophisticated by current or 1998 standards.

RESPONSE provided by Acting Secretary, Department of Justice – continued

Systems Requirements Study completed for CJEP

The report concludes that the systems requirements for CJEP were inadequately specified.

The Systems Requirements Study (SRS) and associated business process documentation completed for CJEP was contributed to by a large number of departmental and agency staff under the guidance of qualified business analysts from an international consultancy firm with a reputation for high quality work in this area. The Department believes that the quality of the resulting documents is objective evidence of a highly effective process which formed a sound basis for development of CJEP systems. This does not imply, however, that every discrete sub process was captured in the initial SRS and business process mapping. It is inevitable that the software development life cycle will be informed by a better understanding of the subtle nuances of processes as it proceeds.

FURTHER comment by the Auditor-General

The department's response does not present any facts which would call into question, or invalidate the audit conclusion. The response presents the department's assertion about the quality of the SRS documents.

Section 3 of the audit report sets out the delays in implementing CJEP and identifies in section 3.3 that inadequate specification of system requirements was one of the factors that contributed to these delays. Section 3.3.2 of the report describes how project participants, stakeholders and the CJEP program director identified weaknesses in the SRS.

Levels of commitment and ownership by partner agencies

The report acknowledges that appropriate governance processes were in place for CJEP but suggests that not all agencies were sufficiently committed to CJEP.

The Department believes that the Audit Report confuses commitment by the various CJEP partner agencies with capacity to devote resources to particular tasks from time to time. The CJEP project extended over the period 1998 until December 2005 and it is inevitable that conflicting demands for resourcing will occur over that timeframe. The Department believes that where resourcing issues were raised with the Steering Committee, they were effectively dealt with.

FURTHER comment by the Auditor-General

The audit conclusion on this matter is that levels of commitment to and ownership of CJEP by partner agencies fluctuated during its implementation. The basis for this conclusion is provided in section 3.3.6 of the report. The department's response validates this audit conclusion.

RESPONSE provided by Acting Secretary, Department of Justice – continued

Benefits Capture and Monitoring Framework

The report concludes that performance indicators relating to intangible benefits are not sufficiently robust.

The Department acknowledges that some performance indicators it has established for CJEP are intangible measures such as better risk management of offenders and better information sharing. The Department believes these to be important measures of the benefits of CJEP, notwithstanding that they are difficult to measure. The Department relies heavily on the experience of departmental staff in the field to determine the extent to which these benefits are being achieved.

FURTHER comment by the Auditor-General

The department's response does not present any facts which would call into question, or invalidate the audit conclusion. In addition, the department's overall response to the report accepts the audit recommendation that it should establish performance measures of a strategic nature that are linked to CJEP's expected outcomes and report performance against baseline data for these measures to both CJEP stakeholders and the Parliament through its annual report.

The Need to Upgrade IT Infrastructure

The report suggests that the need to upgrade IT infrastructure for CJEP should have been included in the initial funding bid.

The Department acknowledged in its initial funding bid for CJEP that it would be likely that further investment in IT infrastructure would be required. Rather than attempt to estimate the extent of this investment at the outset, the Department commissioned a detailed Systems Requirement Study (SRS) and accompanying IT Architecture Study to enable, among other things, a more accurate estimate of the infrastructure investment required. The Department sought and obtained ERC funding of $8m in March 2001, after completion of these studies.

FURTHER comment by the Auditor-General

The report states in section 3.3.3 that the department did not include costs associated with upgrading IT infrastructure in its original budget for CJEP of $14.5 million, but acknowledged that a later funding bid may be needed for infrastructure upgrade funding. This is confirmed by the department's response.

It is a fact that the department was aware at the outset of CJEP that there were significant IT infrastructure challenges across the justice system. This had been recognised in the Pathfinder recommendations. A comprehensive business case would have included at least a preliminary analysis of the likely investment required in IT infrastructure to support the roll-out of planned CJEP systems across the justice system. This work should have been done at the outset of planning for CJEP.

RESPONSE provided by Acting Secretary, Department of Justice

Incremental Funding Approach

The Department acknowledges that additional funding for CJEP was mainly attributable to approved scope changes for the project between 2000 and 2002. The Department does not agree with the audit comment that the funding of $4.5m, approved by ERC in September 2002, should have been foreseen at the inception of CJEP. The need to substantially replace the Corrections Victoria systems was associated with changes in the Corrections Legislative and Policy Framework which did not emerge until 2001/2002.

FURTHER comment by the Auditor-General

It is clear from evidence sighted during the audit that the replacement of elements of Corrections Victoria legacy systems was included in the original scope of CJEP.

*One of the main reasons cited in 2001 for seeking additional funds to substantially replace Corrections legacy systems was that a hybrid E*Justice/PIMS system was used in CJEP Stage 1 which was to be supported by complex messaging and interfaces intended to avoid duplication of data entry and to ensure alignment of the various databases relied upon by Corrections Victoria. This hybrid system was eventually reviewed by Corrections business analysts who highlighted the messaging complexity and difficult trade-offs in user functionality associated with the hybrid system. The potential for issues to arise around the interfaces between the new and legacy systems would have been identified earlier and addressed if CJEP had been adequately planned.*

Completion of CJEP

*All of the IT systems that formed part of CJEP were completed and handed over to the respective agencies by December 2005. The electronic brief module of the E*Justice application continued as a proof of concept in Victoria Police throughout the whole of 2006 and up until June 2007. Victoria Police advised the CJEP Steering Committee in July 2007 that it had decided not to proceed with the user interface for the electronic brief module as it was not consistent with standards for IT systems which had emerged in Victoria Police over the previous two years. Victoria Police also advised that they would be doing a comprehensive review of the processes for creating and managing briefs of evidence and that this review would inform a new user interface for the supporting IT system. Victoria Police further advised that the E*Justice database would still be used for electronic briefs of evidence and that they remain committed to sharing brief information with other Criminal Justice Agencies.*

FURTHER comment by the Auditor-General

*As stated in section 3.1 of the report, the implementation of CJEP is not complete. While four of the five projects comprising CJEP have been delivered, E*Brief, a major module of the Electronic Brief/Disclosure project, is not operating and may not be fully implemented until 2009. E*Brief is a critical component of the CJEP project. The objectives, anticipated functionality and benefits of CJEP cannot be fully realised until E*Brief is operational.*

*E*Brief was part of the approved and funded scope of CJEP. On that basis, the approved and funded scope of the CJEP program had not been fully implemented at the time of the finalisation of this report.*

Auditor-General's reports

Reports tabled during 2007-08

Report title	Date tabled
Program for Students with Disabilities: Program Accountability (2007-08:1)	September 2007
Improving our Schools: Monitoring and Support (2007-08:2)	October 2007
Management of Specific Purpose Funds by Public Health Services (2007-08:3)	October 2007
New Ticketing System Tender (2007-08:4)	October 2007
Public Sector Procurement: Turning Principles into Practice (2007-08:5)	October 2007
Discovering Bendigo Project (2007-08:6)	November 2007
Audits of 2 Major Partnership Victoria Projects (2007-08:7)	November 2007
Parliamentary Appropriations: Output Measures (2007-08:8)	November 2007
Auditor General's Report on the Annual Financial Report of the State of Victoria, 2006-07 (2007-08:9)	November 2007
Funding and Delivery of Two Freeway Upgrade Projects (2007-08:10)	December 2007
Results of Financial Statement Audits for Agencies with 30 June 2007 Balance Dates (2007-08:11)	December 2007
Local Government: Results of the 2006-07 Audits (2007-08:12)	February 2008
Agricultural Research Investment, Monitoring and Review (2007-08:13)	February 2008
Accommodation for People with a Disability (2007-08:14)	March 2008
Records Management in the Victorian Public Sector (2007-08:15)	March 2008
Planning for Water Infrastructure in Victoria (2007-08:16)	April 2008
Delivering Health*SMART*—Victoria's whole-of-health ICT strategy (2007-08:17)	April 2008
Victoria's Planning Framework for Land Use and Development (2007-08:18)	May 2008
Planning Permit Application: Assessment Checklist (2007-08:19)	May 2008
Planning Scheme Amendment: Assessment Checklist (2007-08:20)	May 2008
Patient Safety in Public Hospitals (2007-08:21)	May 2008
Project Rosetta (2007-08:22)	May 2008
Results of Audits for Entities with other than 30 June 2007 Balance Dates (2007-08:23)	May 2008
Review of South East Water's Works Alliance Agreement (2007-08:24)	May 2008
Piping the System (2007-08:25)	May 2008

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

The Victorian Auditor-General's Office website at <www.audit.vic.gov.au> contains a more comprehensive list of all reports issued by the Office. The full text of the reports issued is available at the website. The website also features 'search this site' and 'index of issues contained in reports and publications' facilities that enable users to quickly identify issues of interest that have been commented on by the Auditor-General.

Availability of reports

Copies of all reports issued by the Victorian Auditor-General's Office are available from:

- Information Victoria Bookshop
  505 Little Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: 1300 366 356 (local call cost)
  Fax: +61 3 9603 9920
  Email: <bookshop@dvc.vic.gov.au>

- Victorian Auditor-General's Office
  Level 24, 35 Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: +61 3 8601 7000
  Fax: +61 3 8601 7010
  Email: <comments@audit.vic.gov.au>
  Website: <www.audit.vic.gov.au>